

# **IT Security Products for Business Users**



## **Review of IT Security Suites for Business Users, 2013**

Language: English

September 2013

Last revision date: 16<sup>th</sup> October 2013

[www.av-comparatives.org](http://www.av-comparatives.org)

# Contents



About this review .....	3
Reviewed products .....	6
Management Summary .....	7
Avira Endpoint Security .....	8
Bitdefender Cloud Security for Endpoints .....	13
ESET Endpoint Security .....	17
F-Secure Client Security .....	22
G Data AntiVirus Business with Patch Management .....	28
IKARUS security.manager .....	32
Kaspersky Endpoint Security for Business Advanced .....	36
Sophos Endpoint Security and Control .....	40
Symantec Endpoint Protection .....	44
Webroot SecureAnywhere Endpoint Protection .....	49
Feature lists .....	53

## About this review

Our scenario for AV-Comparatives' 2013 Business Software Review is a single-site company network with a domain controller/file server running Windows Server 2012, and 25 client PCs, running a mix of Windows 8, Windows 7 and Windows XP. A company of this size may well not have a full-time IT manager, so we have considered the management and monitoring of the security software from the point of view of someone who is not highly trained or experienced in IT administration, and only looks after the system part-time. We do however assume that the initial installation/deployment of the software will be carried out by an IT professional who is familiar with small business networks. The increasing availability of hosted Microsoft Exchange services, combined with the fact that Windows Server 2012 has no counterpart to Small Business Server, means that we have not looked at antivirus software for Microsoft Exchange in this year's review.

Although it is a minor point, we start our review of each product by considering how easy it is for the administrator to find the right software components and documentation on the manufacturer's website. It can be time-consuming and frustrating to have to search for all the items needed, or to find that deployment has to be interrupted because a necessary component is missing. The next task for the administrator is to look at the documentation and find the sections relevant to installing the console (where applicable) and deploying the client software. We note here that "quick start guides" can be ideal for these tasks, providing they contain all the necessary details. Comprehensive manuals covering all the features, functions and options of the software need to be properly indexed and bookmarked if the reader is to find a particular section quickly and easily. Regarding installation of the management console on the server (where applicable), we would expect an IT professional to be able to install or update additional components (e.g. SQL Server), open firewall ports or create shares etc. without any assistance. However, should such actions be necessary, we feel that the console's setup program (or the manual) should make very clear exactly what needs to be done.

Even with a network of only 25 client PCs, deploying antivirus software by push installation should be considerably quicker than manually installing on each individual computer. We therefore consider how easy it is to do this with each of the reviewed products; suitable instructions in the manual, describing how to prepare the client PCs for remote installation, are invaluable here. We also look very briefly at installing the antivirus software for the server, which we would expect to be very quick and straightforward.

Once the antivirus software has been deployed, we consider how easy it is to monitor the state of the network using the console. We would expect to be warned clearly of any malware discoveries or potential security risks (e.g. the antivirus software not running or out-of-date on a client PC), and to easily find a means of rectifying any problems. Next we consider carrying out everyday maintenance tasks such as updating and scanning, and (where applicable) how to schedule such jobs.

We then shift our attention to the client antivirus software installed on the PCs. We look at warnings displayed in the event that malware is discovered or that there is a malfunction in the software, and what, if anything, the user is able to do with the program when logged on with a standard user account. We also consider whether the program makes more features available when an administrator account is used. Finally we take a very brief look at the antivirus software that protects the server.

Full details of the points we have looked at for each program are given below:

### Introduction and Software version reviewed

- Overview of the manufacturer's business products, and details of the product reviewed
- Main product version number of each of the components used

### System requirements

- Operating systems supported

### Downloading the software and documentation

- How easy is it to find everything on the website?

### Documentation

- The range of manuals available, scope of each
- How easy is it to find the right document for the job?
- How well is the documentation prepared?
- How easy is it to use?
- Which manuals were used in this test?

### Installing the console

- Are there any difficulties or points of interest?

### Client/server antivirus management interface

- Description of layout and features

### Deploying the antivirus software

- Deployment to clients by push installation
- Are there other installation methods, such as local installation from the client?
- Server protection installation

### Client/server antivirus monitoring

- Status of real-time protection
- Status of signatures (date and time of last update)
- Status of firewall – if applicable
- Program version installed
- Malware discovered and result (e.g. deleted/quarantined) - tested by running AMTSO Feature Settings Check on client
- Software vulnerabilities detected
- Any other relevant information
- Licensing information

### Client/server antivirus tasks (from console)

- Run scans: full, quick, custom – once/automated
- Run a vulnerability scan – once/automated



- Update signatures – once/automated
- Update program version
- Enable/disable components such as real-time protection or firewall
- Add/remove components such as firewall – if applicable
- Add scan exclusion
- USB device control

#### Client antivirus software

- What is visible to the user?
- Are scan/update options available?
- Is there a status display that would alert the user in the event of a problem? If so, can the user easily fix the problem?
- By default, can components be disabled/enabled locally using (1) a Windows domain administrator account (2) a standard domain user account? If the answer to (2) is yes, can configuration options be password protected?
- What happens on malware discovery (AMTSO Feature Settings Check)?
- Is it clear to the user what, if anything, they need to do?

#### Server antivirus software

- Brief description of window
- What functions are available?
- What happens on malware discovery?
- Is there a warning if e.g. real-time protection is disabled?

## Reviewed products

The following manufacturers participated in this review:



The products listed below were reviewed for this report. The manufacturers either provided us with the newest versions of their respective products, or confirmed that the latest version was available from their website (as at September 2013).

- AVIRA Endpoint Security 13.0
- Bitdefender Cloud Security for Endpoints 5.1
- ESET Endpoint Security 5.0
- F-Secure Client Security 11.0
- G DATA AntiVirus Business with Patch Management 12.0
- Ikarus security.manager 4.2
- Kaspersky Endpoint Security for Business Advanced 10.1
- Sophos Endpoint Security and Control 10.2
- Symantec Endpoint Protection 12.1
- Webroot SecureAnywhere Endpoint Protection 8.0

As no major flaws or problems were encountered while reviewing the products, we are pleased to be able to give our Approved Business Product Award to all the participating products.



## Management Summary

**Avira's** mmc-based console and client software will feel very familiar and comfortable to IT professionals, and non-expert administrators will require minimal training. Documentation and client software interface are also of a very high standard. The suite impressed us with its reliable and trouble-free operation in our test.

**Bitdefender** could be deployed by a non-expert administrator due to its cloud-based console and simple local installation process for the endpoint software. The console is simple and straightforward to use.

**ESET** scores very highly with documentation and client software interface. The console is very powerful and can be customised to the administrator's needs. Non-expert administrators may initially require just a little practice to find their way around it.

**F-Secure** allows very detailed monitoring and has an excellent software update monitor to keep track of potential vulnerabilities. We feel that it could be comfortably used by non-expert administrators if some initial configuration is carried out by an IT professional.

**G Data's** clearly laid-out console makes deploying and monitoring client software very straightforward, even if status reporting is not perfect. The minimalist interface to the client software has some obvious advantages for the administrator.

**IKARUS** is very easy to deploy and we liked the ability to reproduce the client software window on the server. The console is essentially fairly practical to use. However, we would say that there are one or two quirks to the software, which may make it more suitable for confident administrators.

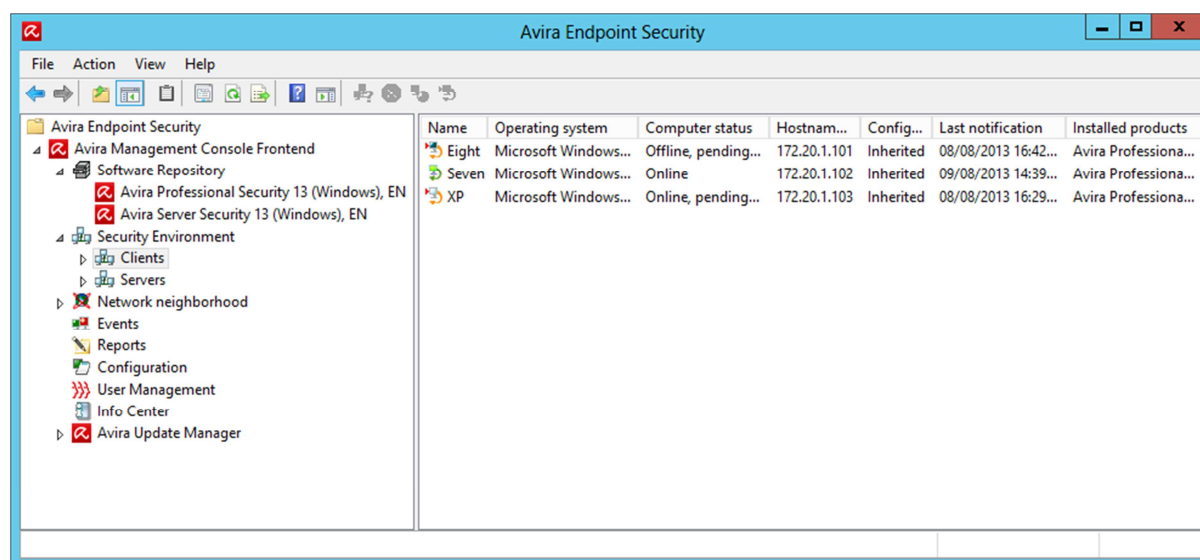
**Kaspersky Lab** use the familiar mmc format and good graphic design to produce a powerful but easy-to-use console. Documentation is generally good, albeit with a couple of minor omissions. Deployment is very straightforward and the real-time progress display is excellent. The client software interface is oriented towards information display for the admin, with no user interaction available by default.

**Sophos'** business software could be used to protect larger networks but is equally well-suited to small business. Installation and deployment should not present a professional administrator with any problems, and the straightforward design of the console makes important tasks and information easy to find. The software worked very efficiently and reliably in our test.

**Symantec's** management console is clear and simple, and good graphic design makes it particularly user-friendly. Client software is practical and familiar, and the deployment process is so simple that a non-expert administrator should be able to do it comfortably. Installation of the console itself is also very easy. In our test, we found the software to be very reliable and unproblematic.

**Webroot** is in many ways ideal for a small business without a full-time system administrator. The cloud-based console requires no installation and enables very simple deployment of client software by local installation on each PC. There are some obvious advantages to the default minimalist user interface.

## Avira Endpoint Security



### Introduction

Avira's small-business software for Windows consists of the Avira Management Console, Avira Professional Security client antivirus software, and Avira Server Security for protecting file servers. For larger and more complicated networks, gateway and Microsoft Exchange Server products are also available.

### Software version reviewed

Avira Management Console 2.07

Avira Professional Security 13.0

Avira Server Security 13.0

### System requirements

According to the avira.com website, Windows Server 2008 and Windows Server 2008 R2, along with their respective Small Business Server variants, are supported server operating systems for the management console. Avira Server Security is additionally supported for Windows Server 2012. Clients can run Windows XP, Vista, and 7, all in 32 and 64-bit versions. In our test, the management console ran perfectly on Windows Server 2012. The antivirus component of Professional Security 2013 is fully compatible with Windows 8, but the firewall is not. The deployment wizard

automatically deselects the Avira Firewall during installation on Windows 8, so that the Windows Firewall is used instead. Avira tell us that the upcoming 2014 version of Professional Security will be fully Windows 8 compatible.

### Downloading the software

We found it very easy to locate the download page for Avira Endpoint Security on the Avira website, and were pleased to see that all the documentation relating not only to the console itself, but also to all possible client software packages, was available for download from the same page:

Product Installation Files					
Avira Endpoint Security	Windows	Aug 1, 2013	EXE	281 MB	📄
Documentation					
User Manual - Avira Professional Security		Jun 27, 2013	PDF	2 MB	📄
User Manual - Avira Server Security		Jun 27, 2013	PDF	903 KB	📄
User Manual - Avira Antivir Windows Server		Aug 30, 2011	PDF	867 KB	📄
User Manual - Avira Management Console		Dec 18, 2012	PDF	7 MB	📄
HowTo - Avira Endpoint Security		Jun 14, 2013	PDF	839 KB	📄
HowTo - Avira Management Console		Feb 12, 2013	PDF	4 MB	📄
User Manual - Avira Antivir Server (Linux)		Jan 23, 2013	PDF	430 KB	📄
HowTo - Avira Server Security (Windows)		Jan 16, 2012	PDF	1 MB	📄
HowTo - Avira Management Console for large networks		Feb 3, 2012	PDF	1 MB	📄
User Manual - Avira Antivir Professional (Linux)		Sep 9, 2010	PDF	481 KB	📄
HowTo - Avira Professional Security (Windows)		Jul 18, 2012	PDF	3 MB	📄

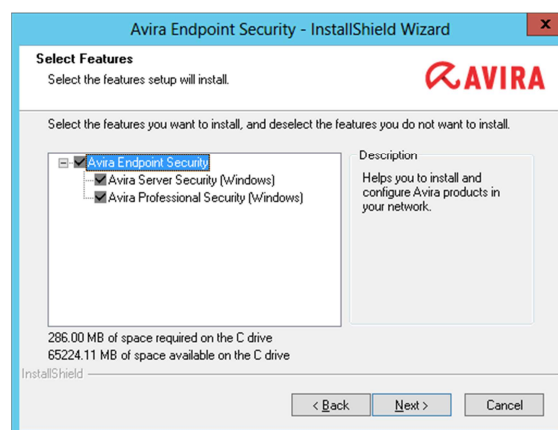
We had assumed that the 281 MB would contain both the client and server software packages, and that we would not need to download these separately, although this turned out to be a mistake.

## Documentation

As can be seen in the screenshot in the previous section, Avira make a comprehensive range of manuals for their small business suite. Each of the three components we used (management console, client protection software, server protection software) has a full manual plus a succinct “How To” guide. We used the How-To guide for the Avira Management Console to assist with installing the console and deploying client software, and found it excellent for this task. There is just the right amount of information for an IT professional; for example, the guide does not go through all the details of installing the console, most of which are very obvious, but does explain how to configure the network settings for larger or more complicated networks. We found the instructions provided for preparing the clients, pushing out the endpoint security software, and carrying out scans and updates, to be clear and straightforward. There is a clickable table of contents at the beginning, and the document has been suitably bookmarked, providing easy access to any section through Adobe Reader’s Bookmarks Bar. Screenshots are used to illustrate the instructions wherever necessary, and there is an explanation of the icons used in the software. We found the How-To guide to be an ideal companion for setting up Avira Endpoint Security.

## Installing the console

Installing the management console on our network was as quick and easy as installing iTunes. Steps included accepting the licence agreement, enter a licence key, choosing the installation folder, selecting a Windows domain account to use for management, and deciding whether to let the program automatically configure the Windows Server Firewall. Setup also asked us whether to include the client and server antivirus packages in the installation, which we accepted.



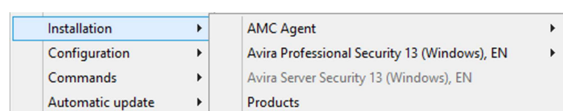
## Client/server antivirus management interface

Avira Endpoint Security uses the Microsoft Management Console framework. The console tree in the left-hand pane displays the main configuration and monitoring items. These are the Software Repository (software packages to be deployed to client and server computers); Security Environment (custom-made groups to which the administrator assigns computers to be managed); Network Neighbourhood (displays the computers on the network using Microsoft’s Active Directory schema); Events; Reports; Configuration; User Management; Info Center (displays news items about the product, e.g. version upgrades); Avira Update Manager, which helps the administrator keep the installed software up to date. Clicking on an item in the left-hand pane displays information and configuration options; right-clicking an item in the tree displays a menu which allows the administrator to go directly to specific tasks and configuration options. The use of the very familiar Microsoft Management Console means that IT professionals and computer enthusiasts will immediately feel at home.

## Deploying the antivirus software

We experienced one very minor glitch/misunderstanding right at the beginning of the deployment process. We had assumed that the security software packages for both the server and the clients had been already been downloaded and integrated into the console, ready for deployment. We were thus rather surprised that when we clicked on

Software Repository, no installation packages were to be seen. This was very easily rectified, however. The How To guide gave clear instructions for importing separate software packages, so we downloaded Avira Server Security and Avira Professional Security from the website, and were able to import these very quickly and easily as explained in the guide. After this minor hiccup, we found the remainder of the deployment process to be exceptionally quick and easy. First, we used the Security Environment to create two groups, one for the clients and one for the server. Next, we installed the Avira Management Console Agent on the clients – this software provides communication between client and server for management and monitoring purposes. This is done by right-clicking the group (or an individual computer), pointing to Installation, AMC Agent, and then clicking Install. The status display in the main pane of the console briefly indicated that installation was underway, and then just a few moments later we could see that installation had successfully completed. We then repeated the process to install the actual security software. We note that once the agent had been installed, the client OS was recognised and the menu entry for the server software was greyed out:



Exactly the same process was used to install Avira Server Security on the server.

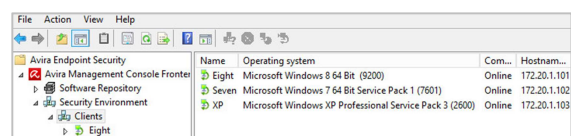
Once we had realised that we needed to import the software packages into the console, we found the remainder of the deployment process to be very intuitive, quick and unproblematic, and our network was protected within a few minutes.

It is possible to perform a local installation on a client PC using the .EXE setup file for Avira Professional Security. Avira do not

recommend installing the agent locally, although their support staff can do this if necessary.

### Client/server antivirus monitoring

Clicking on a group of computers under Security Environment in the left-hand pane of the window displays the status of all the computers in that group. Details shown include computer name, OS, status, IP address, last notification, and products installed.



We could not find a means of displaying the date of the signatures being used or the state of the real-time protection as such. However, if the latter is disabled, the status of the computer concerned will be shown as “Product Error”, and a red exclamation mark will be displayed next to the computer’s name:

Name	Operating system	Computer status
Eight	Microsoft Windows 8 64 Bit...	Online, Product error
Seven	Microsoft Windows 7 64 Bit...	Online
XP	Microsoft Windows XP Prof...	Online

Whilst the specific reason for this is not shown, expanding the computer’s icon in the left-hand pane displays two further icons, for the AMC agent and Avira Professional Security. Clicking on the latter displays a list of events for the software, including (in this case) the fact that real-time protection had been disabled. We do not know what would be displayed here in the event that the service failed to start, or was disabled by malware.

It is also possible to change the view for the Avira Professional Security item, on a per-PC basis, so that it displays the installation/activation status of individual protection components, including real-time protection. If Avira’s client firewall is installed, it is not mentioned separately in



the status display, but events for it are listed along with those for real-time protection:

Avira Endpoint Security	Computer name	Level	Product	Actor	Message
Avira Management Console Frontend	Eight	Warning	Avira Professional Security	Real-Time Protection	Service has been deactivated.
Security Repository	Eight	Warning	Avira Professional Security	Real-Time Protection	Service has been deactivated.
Security Environment	Eight	Warning	Avira Professional Security	Real-Time Protection	Service has been deactivated.
AMC Agent	Eight	Warning	Avira Professional Security	FireWall	Service has been deactivated.
Avira Professional Security	Eight	Warning	Avira Professional Security	FireWall	Service has been deactivated.

Precise version numbers for each of the components of the client software can be found by right-clicking the Avira Professional Security icon for a particular PC, pointing to Views, and selecting Product Version.

Malware discoveries can be seen by clicking on Events in the left-hand pane, which shows all events relating to all computers on the network; alternatively, malware finds and other events for a particular computer can be seen by setting the view of that PC's Avira Professional Security icon to Events. Double-clicking a malware event shows what action was taken (e.g. quarantining).

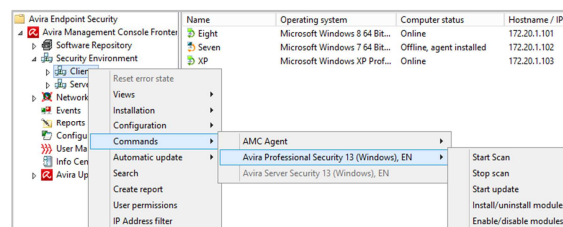
Avira Endpoint Security does not include a vulnerability scan. We could not find any means of displaying licensing information, other than the name of the licence file.

We feel that the simple layout of the Avira Management Console, combined with different views for many items, enables a great deal of information to be displayed without the interface becoming cluttered. However, we found that having to change views to display particular items of information, e.g. software version, was rather inconvenient. We wonder whether Avira might not allow greater customisation of the columns shown, so that it possible for the administrator to display a mix of status, version, event and task items simultaneously, without having to keep switching between views.

### Client/server antivirus tasks

The Avira Management Console allows a wide variety of tasks to be carried out on a single PC or an entire group by right-clicking the group and selecting an item from the context-

menu. As shown in the screenshot below, this can be used to run scans or updates, and install/uninstall or enable/disable components:



To run a scheduled scan, the administrator selects Start Scan from the context menu shown above; the dialog box that then opens allows the scan to be scheduled. Scheduling updates works in exactly the same way.

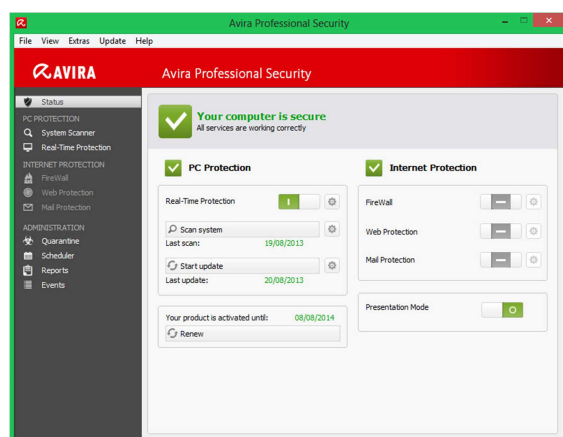
Local access to client software is appropriately controlled by means of Windows administrator privileges, so there is no need for a password-protection feature in the management software. Scan exclusions can be set for all computers, specific groups, or individual computers, by selecting Configuration | Avira Professional Security | Configure from the context menu of the relevant item.

Avira Endpoint Security does not include any means of blocking USB devices.

We understand from reading the manual that the Avira Update Manager automatically updates both the client software already installed, and the software repository (from which the antivirus software is deployed to new clients). There is thus no need to manually update the software version installed on clients.

### Client antivirus software

Avira Professional Security provides the user with a fully featured window, almost identical to Avira's consumer antivirus interface. This even displays licence information:



The user is able to update signatures, run and schedule scans without restriction. There is a very obvious status display, which clearly shows if all is well by means of a suitable icon and text. A standard user is not able to deactivate real-time protection or restore quarantined items (unless administrator credentials are entered at the UAC prompt).

When an attempt is made to download the EICAR test file, Avira Professional Security displays the following alert:



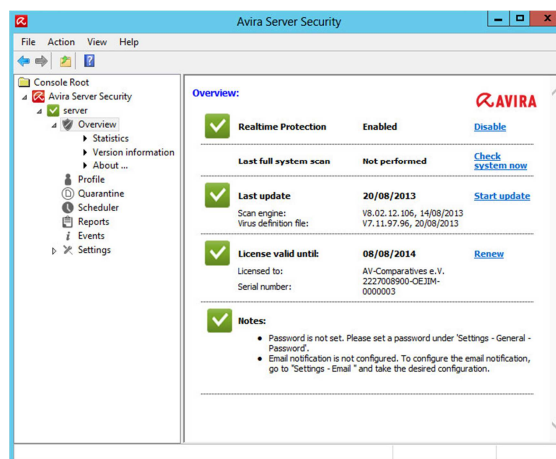
Clicking on Details provides more information on the malware; the only possible action is to quarantine it. A scan is run automatically after malware has been found, and a restart is required after this.

We found Avira Professional Security's interface to be very good. Users can see the

program status and are warned in the event of a problem. They are able to update and scan themselves, but are prevented from taking any risky actions. We feel the alert on malware discovery is appropriate.

### Server antivirus software

Avira Server Security uses the MMC for its interface. Information and tasks displayed on the home page are very similar to the client software.



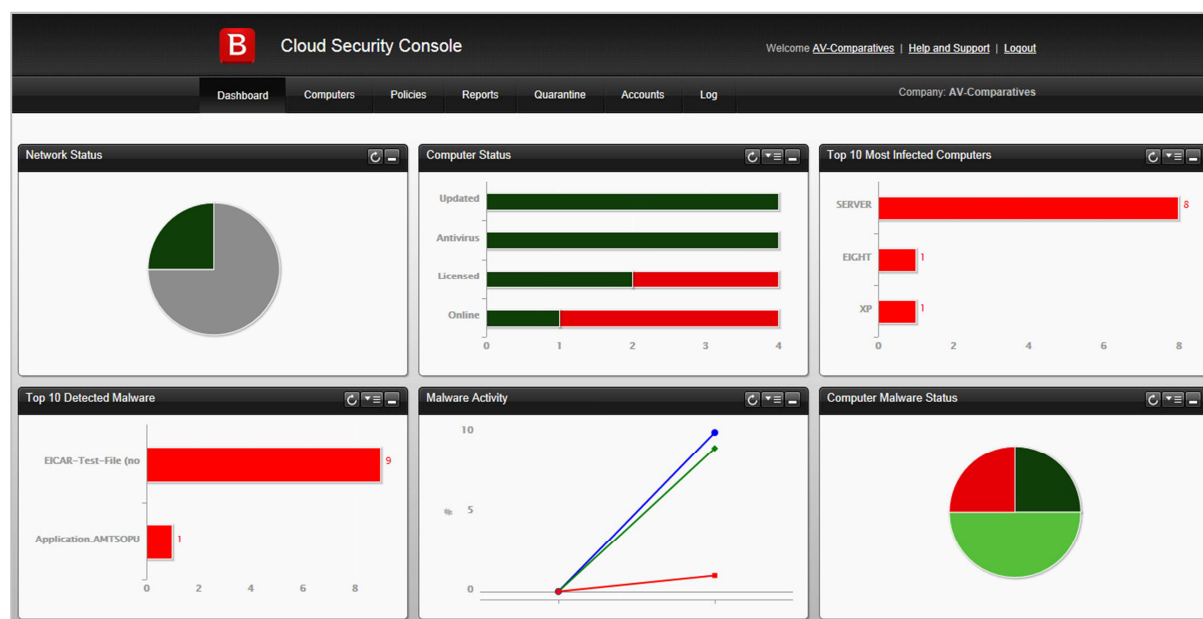
The status display icon and text warn in the event that e.g. real-time protection is deactivated. The EICAR test file was deleted silently when we attempted to download it. The log (Statistics) provides details of the detection.

### Summary

Avira Endpoint Security impressed us with its very straightforward installation, clean interface using the familiar MMC console, and sensible client software. We found the suite to be entirely reliable and trouble-free in operation. Documentation is comprehensive and well produced. Our one suggestion for improvement would be to allow customisation of the client information displayed, in order to minimise the need to switch between views. Overall, we feel that experienced IT professionals should immediately feel at home with the software, and that with a little bit of training it could comfortably be used by non-expert administrators too.



## Bitdefender Cloud Security for Endpoints



### Introduction

Bitdefender make a variety of business products, for companies of all sizes. Cloud Security for Endpoints uses a web-based console to manage antivirus software for client PCs and file servers.

### Software version reviewed

Bitdefender Endpoint Security 5.1.4.227  
 Bitdefender Cloud Security Console as at 21<sup>st</sup> August 2013

### System requirements

Client operating systems: Windows XP, Vista, 7, 8 and 8.1, all 32 and 64-bit versions. We note that Bitdefender Cloud Security also supports Windows Embedded operating systems.

Server operating systems: Windows Server 2003, 2008, 2008 R2, 2012 and 2012 R2, along with Small Business Server variants of these.

### Downloading the software

This is not applicable. Whichever deployment method is used, the software is automatically downloaded as part of the process.

### Documentation

Bitdefender Cloud Security has two manuals for the console, a comprehensive 119-page Administrator's Guide and a succinct 34-page Quick Start Guide. These can very conveniently be downloaded from the Help and Support page of the web console.

Both are clearly written, suitably bookmarked and have clickable contents pages. It is thus very easy to get to a particular page or section. Our one reservation about both documents is the complete lack of screenshots.

We used the Quick Start Guide to help us with the deployment of the client software. We were easily able to find clear instructions for the process in it.

## Installing the console

This is not applicable. The console is web-based, and so merely requires the administrator to open the URL and log in.

## Client/server antivirus management interface

The web console opens in Dashboard view. This shows key information in the form of six boxes: Network Status, Computer Status, Top 10 Most Infected Computers, Top 10 Detected Malware, Malware Activity, and Computer Malware Status. The Network Status box gives a broad overview of the protection status of all the registered computers in the form of a pie chart. Protected computers are shown as green, unprotected as red, offline as grey. This tells the administrator immediately if there are computers that need immediate attention. The Computer Status box provides more details, displaying the separate categories Updated, Antivirus, Licensed and Online, in the form of a bar chart.

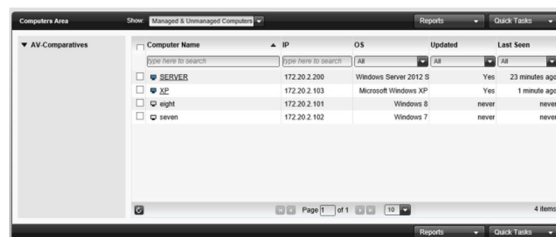
## Deploying the antivirus software

There are two methods of installing the client software on computers: local installation on individual computers, and push installation to a number of computers simultaneously. To install the software locally on a computer, the administrator merely has to log on to the web console and click on Installation Link in the Installation Area.

The installation of client PCs using push installation is clearly described in the Quick Start Guide. The section entitled "Network Discovery Requirements" details the necessary network configuration. We note that this involves setting up a WINS server and configuring clients to use it. Amongst other things, the Computer Browser Service and NetBIOS over TCP/IP have to be activated.

When the network configuration has been completed, the antivirus software has to be locally installed on one PC. Once this has been done, the client PCs to be installed will appear in the Computers view of the console.

Uninstalled computers are distinguished by grey icons and lower-case names:



Clients can then be installed from the console by selecting them and clicking Install Client from the Quick Tasks menu.

In our test, we had some difficulties with the push installation process, and noticed some inconsistencies with the status display of the clients once installed. Bitdefender inform us that this was a one-off glitch due to load issues with the servers used to host the service, and that this has now been resolved.

However, we found that local installation of the software on individual machines was a very quick and easy process, and suggest that this method is probably ideal for smaller networks.

Whether local or push installation used, there is no difference in the respective procedure for client and server computers.

## Client/server antivirus monitoring

The network status pie chart shows at a glance how many of the computers on the network are protected, how many are at risk, and how many are offline. Clicking on this pie chart opens a report with details for each machine, including the status of real-time protection:

Computer Name	IP	General Status	Update Status	Antimalware	License Status	Company Name
SERVER	172.20.2.200	Vulnerable	Updated	Off	Licensed	AV-Comparatives
XP	172.20.2.103	Offline	Updated	On	Licensed	AV-Comparatives
SEVEN	172.20.2.102	Vulnerable	Updated	On	Not licensed	AV-Comparatives
EIGHT	172.20.2.101	Offline	Outdated	On	Not licensed	AV-Comparatives

When we disabled the firewall of one of our test PCs, we did not see any form of warning displayed, or any means of checking the firewall status.

We could not find a way of discovering the version number of the client software from the console, but we understand that the software is automatically kept up to date, so this is not necessary.

Of the six items displayed by default on the console Dashboard page, four relate to malware; together these surely provide enough information about malware attacks for any administrator.

Although we are expecting Bitdefender to add a vulnerability scanner to their business software very soon, we could not find any evidence of this in the version we tested.

Licensing information can be found by clicking on Account/My Account in the console.

### Client/server antivirus tasks

Scans can be run by selecting the machine(s) to be scanned in the Computers view, and clicking Scan in the Quick Tasks menu. A choice of Quick or Full Scan is then offered.

Scheduled scans can be set using a policy, to which a task with details and timing of the scan is added. Scan exclusions are also set here. The same process can be used to enable or disable individual components such as the firewall.

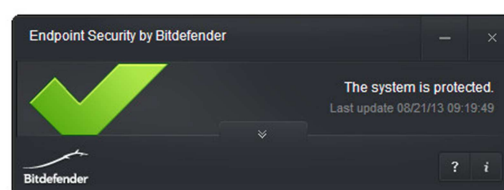
A product/signature update can be carried out by opening the About dialog, which automatically triggers an update.

Components can be installed or uninstalled from the Computers page, Quick Tasks menu, Configure Modules.

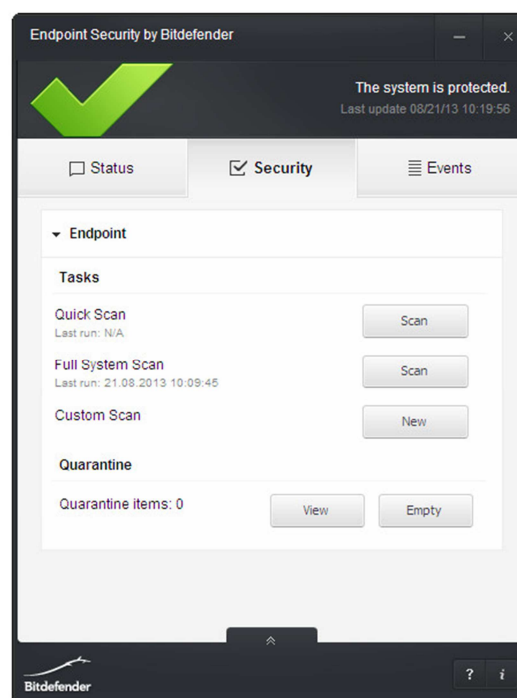
We understand that Bitdefender Cloud Security for Endpoints automatically scans USB devices, but we could not find a means of blocking such devices altogether.

### Client antivirus software

When the main program window of the client software is opened, a minimalist interface, showing nothing more than a status display, appears:

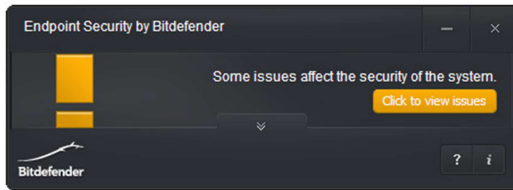


Clicking on the double down-arrow in the centre opens up the interface:



Scan options are clearly accessible on the Security tab. There is no update button.

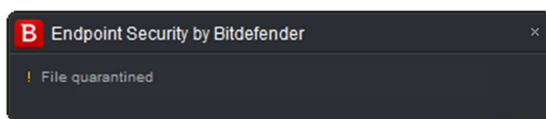
In the event of a problem with the system, the status display changes to a warning:



The “Click to view issues” button opens up a page that explains why there is a warning. In this case, it was because no scan had been run in the last 7 days. There is no “Fix All” button provided, so users have to find a solution themselves.

Even with administrator credentials, the user cannot activate or deactivate components from the client interface; this can only be done from the console.

When we attempted to download the EICAR test file, Bitdefender quarantined the file and displayed the following very simple alert:



We found the essentially simple interface of Bitdefender’s client software to be very suitable for a business environment, albeit with one exception: as the program warns the user in the event of a problem, we feel that a “Fix All” button would be useful, enabling the user to resolve the problem in a single click.

### Server antivirus software

The antivirus software installed on the server is identical to that for the clients, with the exception that only the Antimalware component is installed (not the Content Control or Firewall).

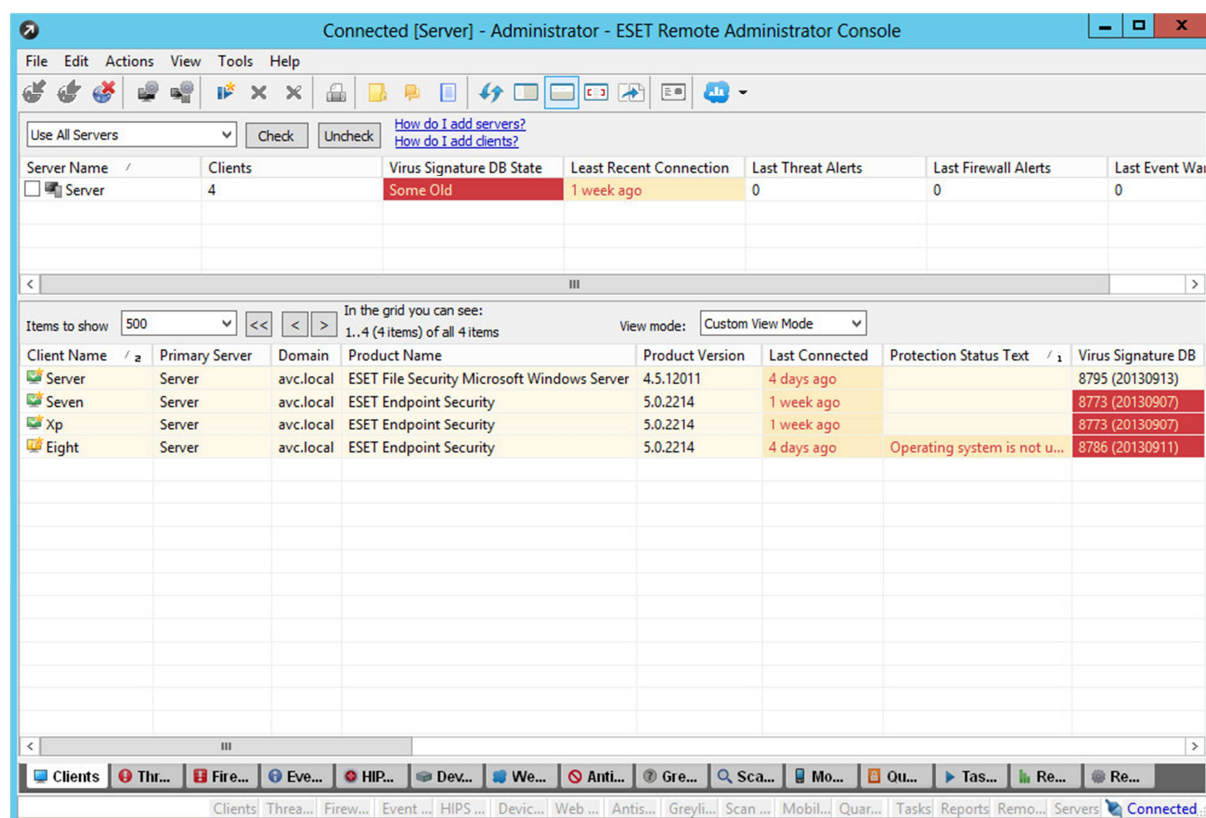
### Summary

Bitdefender Cloud Security for Endpoints could easily be deployed by a non-expert administrator. The web-based console requires no installation or configuration, and installing the client software individually on each PC is quick and simple. We found the console to be

clear and easy to navigate, making it straightforward to find essential information and tasks. The client software is simple and secure but allows users to scan their PCs.

Whilst we experienced a few glitches with the product in our test, we understand that these were caused by a temporary issue with the hosting servers, which has since been resolved.

## ESET Endpoint Security



### Introduction

ESET's business security range includes client antivirus and endpoint protection, mobile security, file and mail server protection, gateway and collaboration security. For our review, we used ESET Endpoint Security client software, and ESET File Security for Windows Server, managed by the Remote Administrator console.

### Software version reviewed

ESET Remote Administrator 5.0

ESET File Security 4.5

ESET Endpoint Security 5.0

### System requirements

ESET Endpoint Security runs on 32 and 64-bit versions of Windows XP, Vista, 7 and 8. ESET File Security runs on 32 and 64-bit versions of Windows Server 2003, 2008, 2008 R2, and 2012, including Small Business Server variants. The ESET Remote Administrator

Server and Console run on all of the client and server versions of Windows listed above.

### Downloading the software

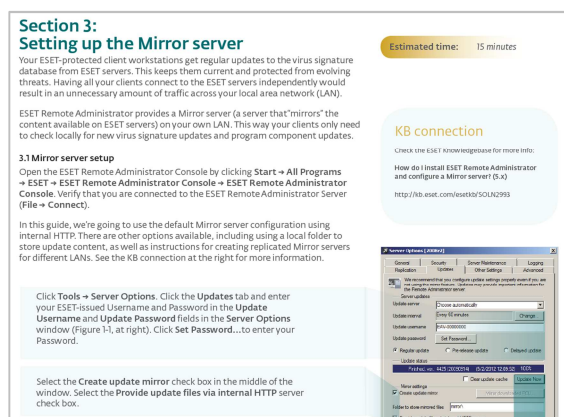
The business downloads section of the ESET website presents a clear overview of all the products, making it easy to find the item you want. The individual download page for each product also includes links to all the relevant documentation for the product.

### Documentation

ESET produce two manuals for Remote Administrator, a very comprehensive 122-page User Guide, and a succinct 13-page Quick Start Guide. Both are produced to extremely high professional standards, being well written and organised, but also clearly illustrated, laid out and easily accessible. There are clickable contents pages and extensive bookmarking, making it very easy to get to a particular page or section. Both

documents are well illustrated with screenshots.

We were particularly impressed with the Quick Start Guide, aka Basic Setup Guide. It provides exactly the right amount of information needed to get the console and client software up and running – even starting with purchasing and downloading the software. We especially liked the way the guide integrates its instructions with the screenshots, using a translucent blue overlay to connect the text on the left with the screenshot on the right:



We note that ESET also state the estimated time needed for each particular configuration job, and provide clickable links within the .pdf document to the online knowledge base. We can only describe the Basic Setup Guide as outstanding. As it is only 13 pages long including cover and contents pages, we would recommend that administrators read the whole thing before starting installation and deployment.

### Installing the console

There are two steps to installing ESET Remote Administrator. The Server component provides the actual functionality, while the Console is the management interface. The Console can be installed on a different computer from the Server, or on multiple computers, or even run from a USB portable drive. Installing the Server component involves accepting a licence agreement, importing a licence key (provided

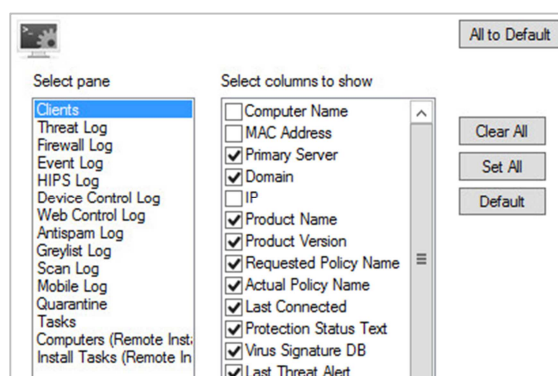
by ESET), entering passwords for various functions, and entering the username and password required to download updates (also provided by ESET). Setting up the Console merely requires the location of the installation folder to be decided.

We found the installation process to be very straightforward.

### Client/server antivirus management interface

The layout of the ESET Remote Administrator console is fairly similar to Microsoft's MMC consoles. There is a menu bar and toolbar along the top, with a narrow left-hand pane and larger right-hand pane. Additionally, a row of tabs along the bottom of the window allows a wide variety of views to be shown in the main pane, including Clients, Threats, Quarantine, Tasks, Reports, Remote Install, and various logs. We initially found that it was not easy to obtain an overview, given the array of available tabs, buttons, menus and links. However, with a little practice, essential views and tasks can be found.

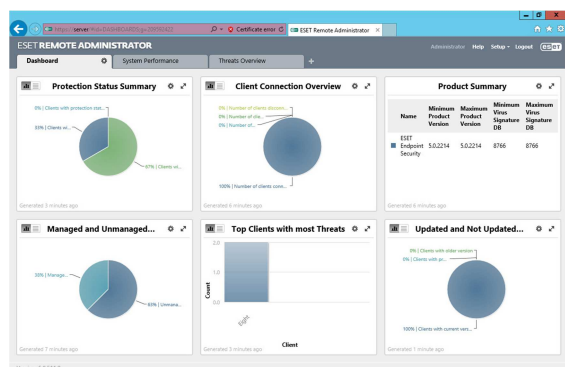
We note that the content of all the pages of the console can be customised extensively. The order of the columns can be changed easily by drag and drop, and the columns to be displayed can be added or removed:



We find this very useful, as it allows administrators to display exactly the information they consider most important.



As well as the standard Windows-based console, ESET also provide a web-based console. This does not allow administrative tasks to be carried out, but is very valuable for monitoring, especially as it is highly customisable. The content of each of the boxes shown can be chosen individually; the screenshot below shows a custom dashboard we made:



We feel the design of the web console is very clean, simple and modern, in contrast with the Windows-based console, which seems complicated and rather old-fashioned in comparison. We would suggest that if ESET could build administrative tasks into the web console, and allowed the display of these to be customised too, an unbeatably clear but powerful console might result.

### Deploying the antivirus software

Deployment of the client software involves creating installation packages from the 32 and 64-bit .MSI installers. This can be performed as a separate task, or as part of the first push installation (it only needs to be done once). The administrator then clicks Default Search Task in the Remote Install Pane, selects the client machine(s) to be installed, and selects Windows Push Installation from the Actions menu. Progress can be seen in the Tasks pane.

We would suggest that administrators new to ESET Remote Administrator might need a little assistance in finding their way around the console at first. However, the Basic Setup

Guide provides exactly that; we used the guide to assist us with deployment, and found it to be a very straightforward procedure.

As an alternative to push installation, the administrator can create an installation package for local installation, which is then run on individual client PCs.

ESET produce a separate product to protect file servers, ESET File Security. The installation process is however identical to that of the client software, involving the creation of the relevant installation package and distribution by push install or local installation.

### Client/server antivirus monitoring

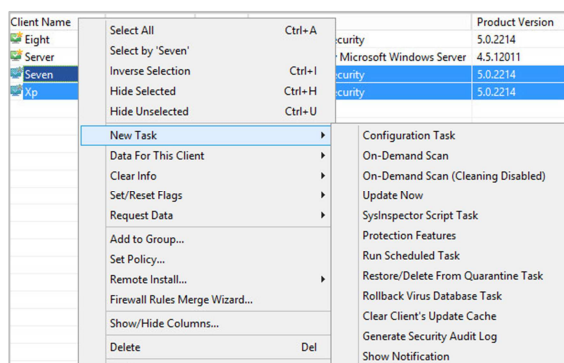
The Clients page of the ESET Remote Administrator console displays a great deal of information about monitored computers. Protection Status Text shows the state of important protection components such as real-time protection and firewall, as displayed in the window of the client software. We find this very good, as it tells the administrator not only that something is wrong, but also the exact nature of the problem. Other items shown in the window are the version of the virus signature database being used by each machine, along with its date; product name and version number of the software installed; and last malware discovery (further details can be seen in the threats pane).

The License Manager in the tools menu shows the licence being currently used, the number of client licences in total and those being used.

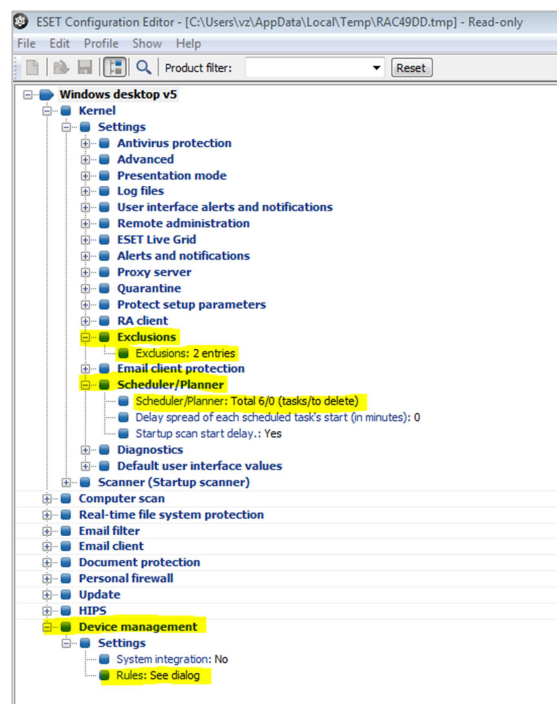
Both the Clients view of Remote Administrator console and the client software itself will indicate if important Microsoft updates are available (see main screenshot at the start of the section). There is however no other form of vulnerability scan.

## Client/server antivirus tasks

Right-clicking one or more selected computers in the Clients tab allows a number of different tasks to be started from the New Task sub-menu. These include full or custom scans, updates, and activating or deactivating specific components such as real-time protection.

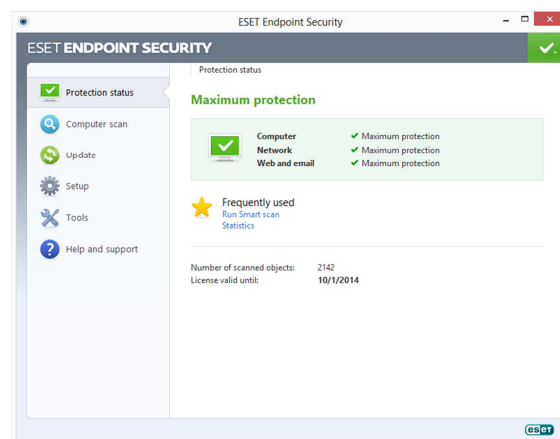


The administrator can choose to deselect the ESET firewall during deployment and use Windows Firewall instead. Additionally, the Configuration Task dialog contains exactly the same range of options as is available in the client software itself; this includes completely disabling the firewall. The program version can be updated using the Upgrade Windows Client entry in the Remote Install Wizard. Scheduling scan and signature updates, adding scanning exclusions, and USB control are all performed using the Configuration Editor:



## Client antivirus software

ESET Endpoint Security uses the same interface as ESET's consumer antivirus software, which we regard as a model of simplicity and clarity.

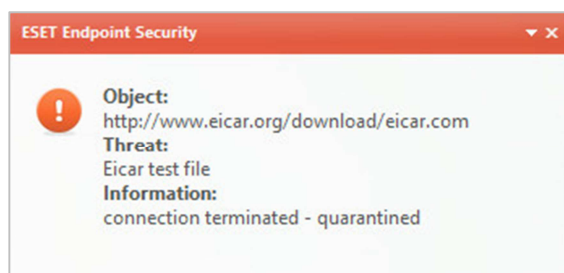


There is a very obvious status display in the form of a green text heading plus tick (checkmark) symbol when all is well; in the event of a problem, the text turns red and becomes a warning message, while the symbol changes to an exclamation mark. Update and scan options are easily accessible from the menu bar on the left-hand side. It is not possible to disable protection components such as real-time protection when using a



standard user account (unless administrator credentials are entered at the UAC prompt).

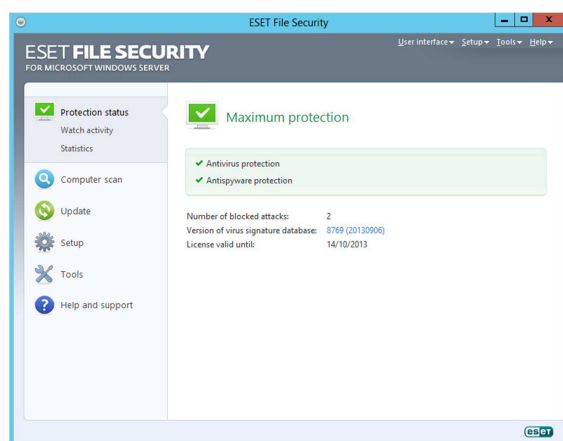
When we tried to download the EICAR test file, ESET blocked the download and displayed this warning message:



We feel this makes reasonably clear to the user that no further action is required.

### Server antivirus software

In terms of the user interface, the file server antivirus software can be regarded as identical to the client endpoint protection, except that the firewall and email protection are not included:

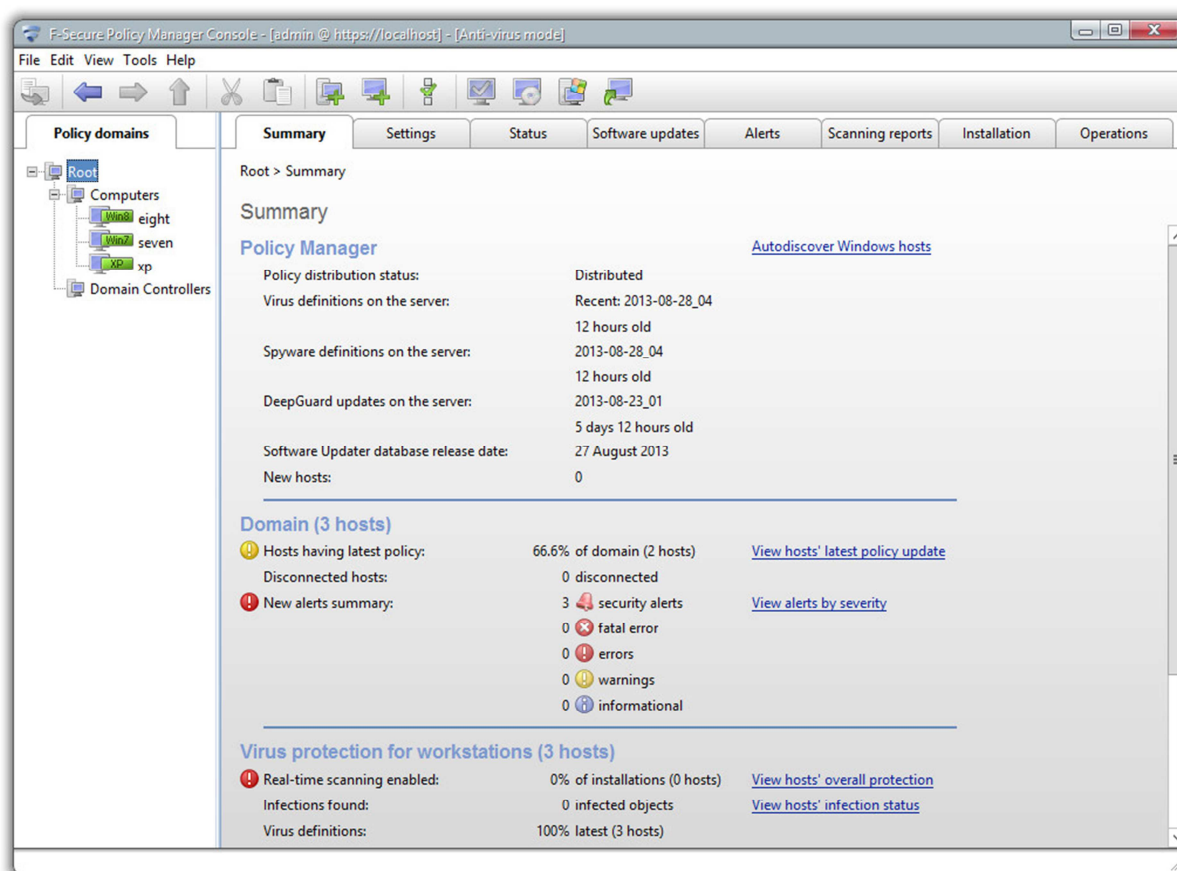


### Summary

We found many aspects of ESET's business product to be outstanding. We regard the client software, web console and documentation, especially the Basic Setup Guide, as exemplary. The Windows-based console is very powerful, and certainly quite useable with a little bit of practice; it seems well suited to larger business networks. However, for a small business, it appears

complicated and rather old-fashioned in comparison with its web-based counterpart. We feel that if ESET could integrate management tasks into the web console (which can currently only be used for monitoring), an unbeatably clear and simple small-business package would result.

## F-Secure Client Security



### Introduction

F-Secure provide businesses with two protection models, a hosted security service and a self-managed business software suite. We tested the latter. It consists of a management server and console called Policy Manager, endpoint software called Client Security, and server antivirus software called Server Security.

### Software version reviewed

F-Secure Policy Manager 11.0

F-Secure Server Security 10.0

F-Secure Client Security 11.0

### System requirements

F-Secure Policy Manager runs on Windows Server 2003, 2008, 2008 R2 and 2012. F-Secure Client Security runs on Windows XP, Vista, 7 and 8; with the exception of Windows XP (32-bit only), both 32 and 64-bit versions

are supported. Server Security runs on all versions of Windows Server from 2003 to 2012, with the latest version, 10.1, also supporting Windows Server 2012 R2.

### Downloading the software

The Business Downloads section of the F-Secure website provides a clear overview of the components of the Business Suite; clicking on the link for any component opens a details page with the respective system requirements and download links for the software and documentation.

### Documentation

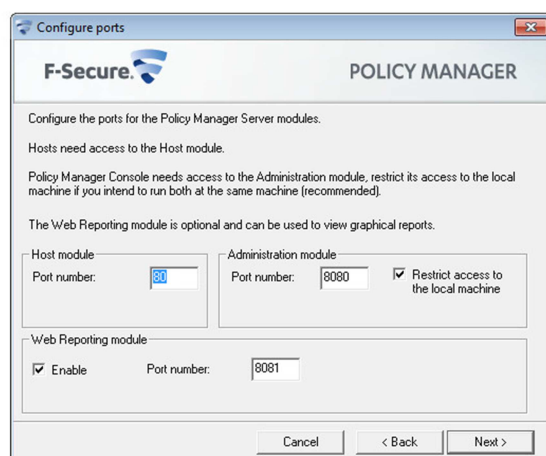
F-Secure provide a comprehensive 157-page guide to the Policy Manager, which covers all aspects of installation, deployment and management. It has been produced to a high standard, is suitably bookmarked, and has a clickable contents page, making it easy to get

to a particular section quickly. Unfortunately, it is completely lacking in screenshots.

There is also a 20-page Quick Installation Guide, covering installation of the console and deployment of the client software. This is also very well produced and has the advantage of being well illustrated with appropriate screenshots. We used this to help us with the installation and deployment processes, and found it excellent, with one exception; please see the note in the next section regarding Windows Server Firewall.

### Installing the console

Installation of the console is as quick and easy as installing iTunes. There is a choice of languages, a licence agreement to accept, the choice of installation folder location and ports to be used for the different console modules.



We note that the standard ports used for the Policy Manager are not opened by default on Windows Server operating systems. Whilst an experienced administrator would realise this and take appropriate action, we note that there is no warning in the setup wizard that these ports will need to be opened manually. We were also unable to find anything about this in either of the relevant manuals.

However, F-Secure tell us that they are aware of this, and are taking steps to amend the manual accordingly.

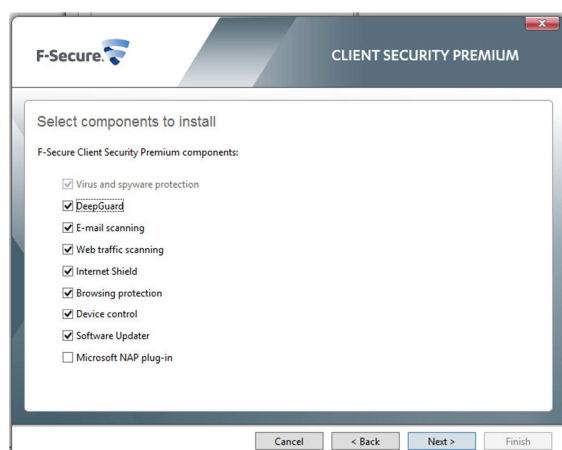
### Client/server antivirus management interface

The F-Secure Policy Manager console uses a two-pane window similar in design to Microsoft's mmc consoles. The narrow left-hand pane displays computers in groups; individual computers or entire groups can be selected, the details of which are then shown in the right-hand pane.

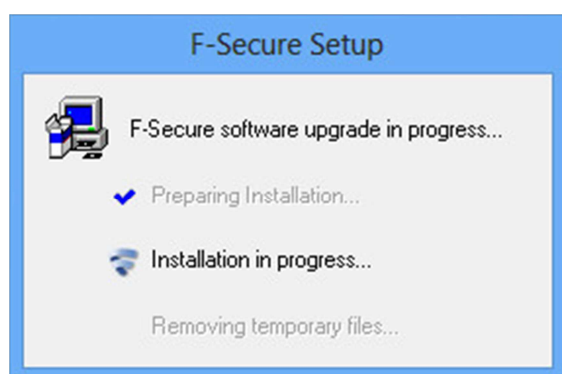
There are a number of tabs along the top of the main right-hand pane. Summary (shown above) displays an overview of the state of the network, with red or yellow icons warning of problems. The Settings tab allows the client software to be configured, while the Status section provides very detailed information on the state of every component of every client. Software updates is a vulnerability monitor which checks for updates in Windows and other third-party software. Alerts shows malware detections, Scanning Reports displays scan logs, Installation allows endpoint protection software to be deployed to client PCs, and finally Operations allows update and scan tasks to be carried out. We found the layout of the console to be essentially clear and easy to navigate.

### Deploying the antivirus software

We found the deployment of the endpoint software to clients by push installation to be a very straightforward process. The wizard uses autodiscover to detect Windows PCs on the network, which can then be selected for installation. Appropriate software packages have to be imported the first time the wizard is used; there is one for clients, and one for servers, both cover 32 and 64-bit architectures. The individual components to be installed can easily be selected:



There is a choice of languages for the UI, and the option of automatically uninstalling any conflicting antivirus software. Finally, options for restarting the client PC after installation can be set. The installation process can be seen on client PCs:



A message box informing the user that the client PC should be restarted appeared at the end of the installation process, as we specified in the deployment wizard. The console also shows that installation is complete.

Alternative installation methods are available. The client security packages can also be installed by policy, or locally on each client PC, using an MSI installation package created in the console.

Server protection installation can be carried out locally with the MSI package, or by push installation from the console. The procedure is identical to clients but uses a different software package.

## Client/server antivirus monitoring

The status of real-time protection can be seen in the Status tab under Overall Protection:

Root > Computers > Status > Overall protection

Overall protection

Hosts: 3 (0 selected)

Host	Real-time scanning	Internet Shield security level	Incoming e-mail scanning	Outgoing e-mail scanning
Win8 eight	Disabled	Office	Enabled	Enabled
Win7 seven	Disabled	Office	Enabled	Enabled
Win xp	Disabled	Office	Enabled	Enabled

To reorder columns, drag column headers.  
To hide/show columns, right-click on a column header.  
To sort by a column, left-click on a column header.

The list of components monitored is comprehensive, with Internet Shield (firewall), ingoing and outgoing email protection, Exploit Shield and Software Updater all shown. We also liked the fact that it is possible to re-order or hide the columns, and sort the table by a particular column. In our test, we found that the status of real-time protection displayed in the console was slow to react, taking 10 minutes to react after the change had registered on the client. However, this setting can be changed to as little as 5 seconds.

The Automatic Updates view of the Status tab shows the time of the last signature update and the version installed.

The program version installed can be seen in the Installed Software view of the Status tab. This also indicates which components of the software (e.g. firewall) are installed.

Malware detections and action taken can be seen under the Alerts tab.

We were particularly impressed with F-Secure's Software Update monitor. This displays a complete list of available updates for the operating system and also third-party software.

Software updates			
Missing updates		Configure Software Updates	
Category	Software	Update description	CVE ID
Critical security	Adobe Flash 5 Gold	Security updates available for Adobe Flash Player	
Critical security	Windows Media Player 9.0 Gold	Vulnerability in Windows Media Format Runtime Could Allow Remote Co...	CVE-2013-3127
Important security	Microsoft Visual C++ 2008 SP1 Redistributab...	Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Re...	CVE-2010-3190
Important security	Windows 7 Professional (x64) SP1	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (283...	CVE-2013-2556
Important security	Windows XP Professional SP3	Vulnerability in Windows Internet Printing Service Could Allow Remote C...	CVE-2008-1446
Non-security	.NET Framework 4 Client (x64) Gold	Update for Microsoft .NET Framework: June 2013	
Non-security	.NET Framework 4 Client Gold	Reliability Update 2 for the .NET Framework 4	
Non-security	.NET Framework 4 Client Gold	Update for Microsoft .NET Framework: June 2013	
Non-security	Internet Explorer 8 Gold	Fix for issue: Array elements in very large loops may be returned as undef...	
Non-security	Windows 7 Professional (x64) SP1	Windows Media Player 12 displays scrambled DVD content in Windows 7...	
Non-security	Windows 7 Professional (x64) SP1	An update is available that adds support for DTLS in Windows 7 SP1 and...	
Non-security	Windows 7 Professional (x64) SP1	An enterprise hotfix rollup is available for Windows 7 SP1 and Windows 8...	
Non-security	Windows 7 Professional (x64) SP1	Update for Microsoft .NET Framework: June 2013	
Non-security	Windows 7 Professional (x64) SP1	Telugu characters are not displayed correctly in the Nirmala UI font in Wi...	
Non-security	Windows 8 Professional (x64) Gold	Windows RT, Windows 8, and Windows Server 2012 update rollup: Augus...	
Non-security	Windows 8 Professional (x64) Gold	A microcode update is available for Windows 8-based computers that us...	
Non-security	Windows XP Professional SP3	Information about new Group Policy preferences in Windows Server 2008	
Non-security	Windows XP Professional SP3	When you disable and then re-enable the LAN-side network adapter on a...	

There is a link to the configuration page for the Software Updater, which allows updates to be installed automatically. However, exclusions are possible in the event that the administrator needs to block the installation of a particular patch. Manual updates can also be made.

Licensing information is not displayed in the console; F-Secure inform us that it is not possible with the licence model they use for business products.

### Client/server antivirus tasks

Both updates and scans can be started from the extremely simply designed Operations tab. Policy Manager automatically checks for outdated software, so running a vulnerability scan is not necessary. The Software Updater in Settings can be used to automatically install software updates.

Individual components of the software, such as real-time protection or firewall, can easily be disabled from the Settings tab.

Components of the suite can be added or removed by rerunning the installation wizard. USB device control is configured by policy, using the table shown below:

Hardware Devices			
<input type="checkbox"/> Disallow user changes			
Active	Display Name	HardwareID	Access Level
Yes	USB Mass Stor...	USB\Class_08	Full access
Yes	Wireless devices	USB\Class_E0	Full access
Yes	DVD/CD-ROM...	gencdrom	Full access
Yes	Windows CE ...	{25dbce51-6...	Full access
Yes	Floppy drives	{4D36E980-E...	Full access
Yes	Modems	{4d36e96d-e...	Full access
Yes	COM & LPT p...	{4d36e978-e...	Full access
Yes	Printers	{4d36e979-e...	Full access
Yes	Smart Card Re...	{50dd5230-...	Full access
Yes	Imaging Devic...	{6BDD1FC6-...	Full access
Yes	IEEE 1394 Host...	{6bdd1fc1-8...	Full access
Yes	IrDA Devices	{6bdd1fc5-8...	Full access
Add		Edit	

Clicking on an item and then clicking Edit allows the device type to be set to Block. We found this very simple and convenient.

The program version can be updated by creating a new installation package with the updated software, and then pushing it out by policy; this is done by clicking the Installation tab, and then Install under Policy-based installations.

Scanning exclusions for real-time protection and on-demand scans are set by policy:

File Scanning	
Scan Files = Files with These Extensions	
Decide Action Automatically = Enabled	
Action on Infection = Ask After Scan	
Scan Network Drives = Enabled	
Scan when Renamed = Enabled	
Scan Inside Archives = Disabled	
Inclusions and Exclusions	
Included Extensions = COM EXE SYS OV? BI	
Included Extensions for Compressed Files =	
Add Extensions Defined in Database Update	
Excluded Extensions Enabled = Disabled	
Excluded Extensions	
Excluded Objects Enabled = Disabled	
Excluded Objects	
Excluded Processes Enabled = Disabled	
Excluded Processes	

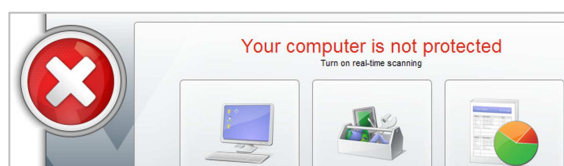
### Client antivirus software

The client endpoint software has a System Tray icon and a fully featured interface, very similar to F-Secure's consumer security products:





The user can run updates and full or custom scans from the smaller buttons along the bottom of the window. There is a status display in the form of a text title and symbol at the top of the window; these change to display a very obvious warning in the event of a problem:



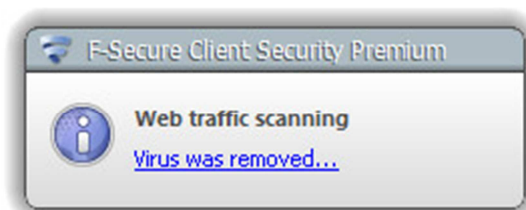
We note that no easy way is provided to correct any problems shown by the status display; there is no Fix-All button or equivalent. We also found that if the real-time protection is disabled from the console, the status display in the client software continues to show "Your computer is protected", even though Windows Action Center is warning that antivirus and antispyware protection is turned off. F-Secure tell us that this is by design, as the product is managed by the administrator and users should not be disturbed by security alerts.

We were pleased to see that the status display does warn of vulnerabilities, with the text "Critical software updates missing" below the main status text.

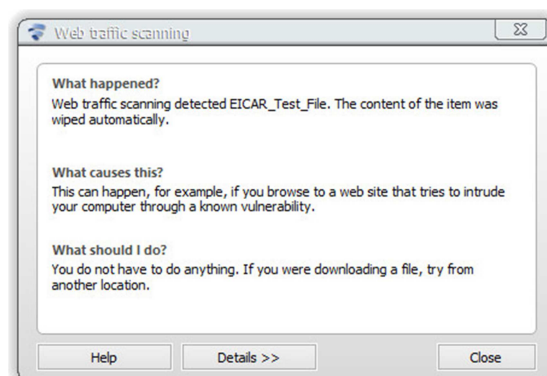
When we logged on to our test PC with a standard user account, we were able to deactivate the real-time protection of F-Secure Client Security without any form of

challenge. It is possible to prevent user changes in the console, by allowing only administrator accounts to make alterations to the settings; we suggest this would be a better default setting.

When an attempt was made to download the EICAR test file, F-Secure Client Security blocked the download and displayed the following pop-up:



This makes clear that the virus has been removed, so the user should not have to worry about taking any action. Clicking on the text shows more information:



The Details button additionally displays the name of the item, malware type, and web address from which it originated. We can only describe F-Secure's warnings on malware discovery as exemplary, starting with a very simple but clear message box, but allowing users to see more information if necessary.

### Server antivirus software

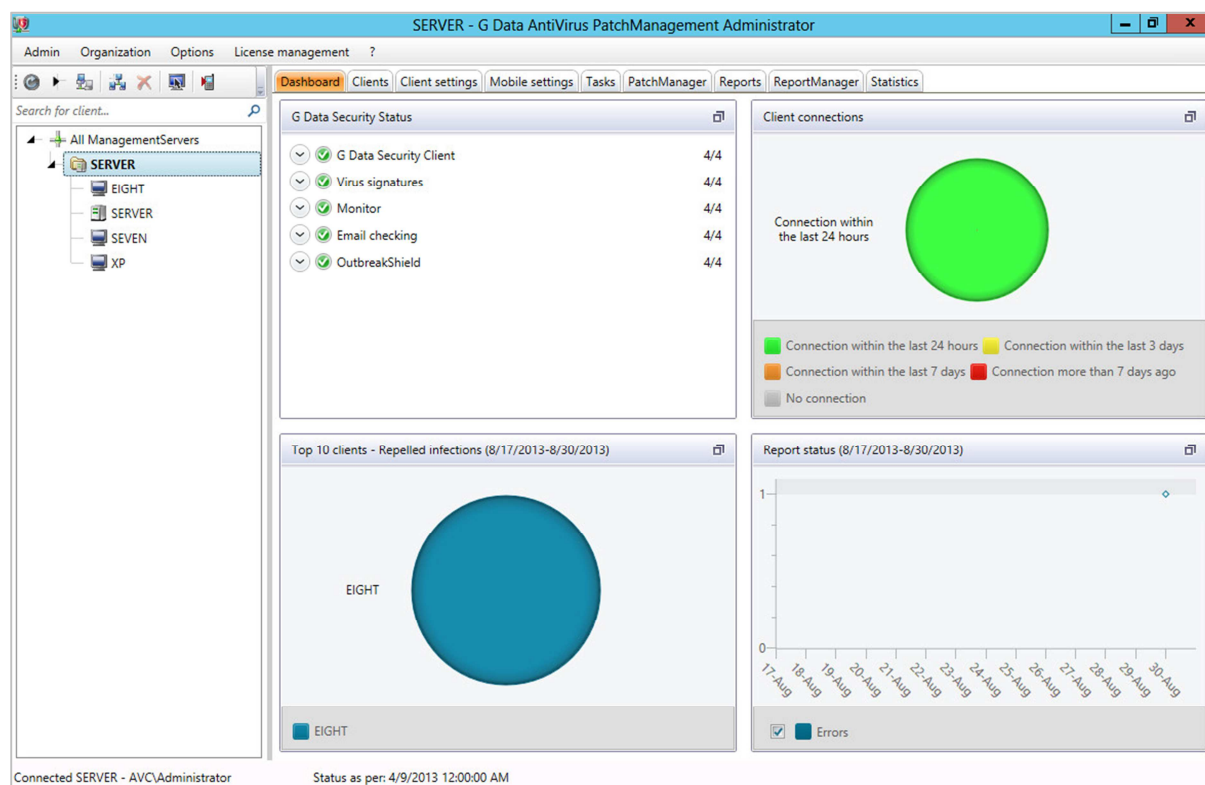
The server protection has a familiar F-Secure System Tray icon. This can be right-clicked to display a context menu of scanning options. There is no program window, however; other tasks are carried out by means of a web

console. Whilst this provides the same functionality as a more standard Windows-based interface, we did not find it very easy to use and suggest that it is more suited to IT professionals than non-expert administrators. F-Secure tell us that it was developed for use with the Windows Server Core configuration, which does not have a graphical user interface.

### Summary

F-Secure's business suite is in many ways very well designed. Installation and deployment are very straightforward, as long as the need to open firewall ports is understood. The console and client software are essentially well designed and easy to use. Monitoring of protection features in the clients is very detailed, and malware alerts on client PCs are excellent. The Software Update monitor is outstanding. We do however have some reservations about the default settings. We would suggest that a faster polling interval would provide a more accurate status display, and that user access to protection settings should be blocked as standard. We conclude that the software is essentially well designed, but could be made more suitable for non-expert users if configured by an IT professional first. F-Secure tell us that they provide free training for partners and customers to assist with setting up and using the product.

## G Data AntiVirus Business with Patch Management



### Introduction

G Data make a variety of security software products for businesses of all sizes. We tested Antivirus Business, a straightforward antivirus solution for small businesses, managed by the G Data Administrator Console. The package we used also included the Patch Management feature, which is available as an add-on for any G Data business solution.

### Software version reviewed

G Data Administrator 12.0

G Data Security Client 12.0

### System requirements

G Data Antivirus Business is supported on clients with Windows XP (32-bit only), Windows Vista, 7 and 8, and servers with Windows Server 2003, 2008, 2008 R2, and 2012. We note that under some circumstances, a glitch related to SQL Server may occur if the console is installed on a Windows Server 2012 domain controller. This

prevents the user from logging on to the management console, but is quickly and easily fixed by G Data Support.

### Downloading the software

The software and manual are downloaded by means of a link in an email sent by G Data.

### Documentation

G Data make one manual covering the installation, configuration and management of the entire suite, i.e. console and client software. It is comprehensive, at 181 pages, and produced to a very high standard. The contents page is very simple, listing only major sections of the document, but it is clickable. The manual has been extensively bookmarked, so it is easy to get to a specific page or section from Adobe Reader's Bookmarks Bar. There are appropriate screenshots to illustrate major features and tasks. We feel the manual is well written and sensibly organised.



## Installing the console

We found the installation of G Data Administrator a very quick and easy process. Running the setup wizard involves accepting the licence agreement, choosing an installation folder, stating whether the machine being installed is a primary or secondary server, and installing SQL Server Express. The latter step is recommended for up to 1000 clients, and is carried out automatically by the wizard.

## Client/server antivirus management interface

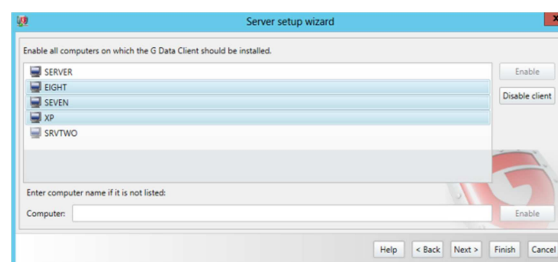
The layout of the management console is similar to Microsoft's MMC consoles. A narrow left-hand pane shows the management server and its associated client/server machines. Clicking on an individual computer in this pane can display information about it in the right-hand pane, whilst clicking on the server at the top of the tree will display details of the whole network.

By default, the right-hand pane shows the Dashboard. This includes a summary of security details (real-time protection, update status, installation status of client software). Other panels show malware infections and client connections in the form of pie charts, while a fourth quadrant shows report status. We feel this provides a very clear overview of the most important security information.

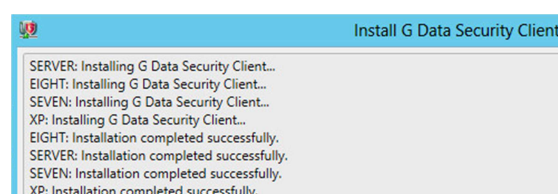
Tabs along the top of the right-hand pane allow the view to be changed to show items such as detailed information about clients, configuration settings for the software, software updates available for Microsoft and other third-party vendors, and malware detections.

## Deploying the antivirus software

When the administrator logs in to the console for the first time, a deployment wizard starts automatically. This is remarkably simple, and merely involves selecting the machines to be installed from a list of computers found on the network:



We note that client PCs and servers can be installed together, there is one installation package used for both. After a few simple configuration steps, the wizard proceeds, and after just a couple of minutes, the status display informs the administrator that installation was successful:



We found G Data's deployment process to be exceptionally quick and easy.

The G Data Security Client can also be installed locally on individual PCs, or by creating an installation package that is distributed by logon script.

## Client/server antivirus monitoring

The status of updates and real-time protection can be seen in the Security Status box of the Dashboard (home) page of the console. We note that if a PC's real-time protection is disabled from the console, or permanently disabled on from client, the Dashboard will immediately show that it is not running on the relevant machine. However, if it is "temporarily" disabled (up to 8 hours) from the System Tray icon of the client, this is not shown in the console, which continues to report that all is well. We are concerned that if malware were able to mimic this particular action, the administrator would not be made aware of it. Administrators may be best advised to leave RTP locked down on the client and only change it in the console.

The program version installed is shown in the Clients view.

Malware discoveries are individually listed in the Reports view, and an overview of infected machines is displayed on the Dashboard.

Available software updates, i.e. patches for vulnerabilities, are shown in detail in the Patch Manager view. This can be sorted according to patch, client, vendor or product:

Drag the column header to this area to group by this column.

Patch	Client	Vendor	Prod
MS13-004 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (KB2742598)	EIGHT	Microsoft Corp.	Win
MS13-004 Security Update for Microsoft .NET Framework 3.5.1 on Win7 and 2008 R2 SP1 x64 (KB2756921)	EIGHT	Microsoft Corp.	Win
MS13-004 Security Update for Microsoft .NET Framework 4 on XP, Vista, Win7, 2008, 2008 R2 x64 (KB2742595)	EIGHT	Microsoft Corp.	Win
MS13-005 Security Update for Windows 7 x64 (KB2778930)	EIGHT	Microsoft Corp.	Win
MS13-005 Security Update for Windows 7 x64 (KB2785220)	EIGHT	Microsoft Corp.	Win
MS13-007 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (KB2736418)	EIGHT	Microsoft Corp.	Win
MS13-007 Security Update for Microsoft .NET Framework 3.5.1 on Win7 and 2008 R2 SP1 x64 (KB2736422)	EIGHT	Microsoft Corp.	Win
MS13-008 Security Update for Internet Explorer 8 for Windows 7 x64 (KB2799329)	EIGHT	Microsoft Corp.	Win
MS13-009 Security Update for Microsoft .NET Framework 4 on XP, Vista, Win7, 2008, 2008 R2 x64 (KB2736428)	EIGHT	Microsoft Corp.	Win
MS13-009 Cumulative Security Update for Internet Explorer 8 for Windows 7 x64 (KB2792100)	EIGHT	Microsoft Corp.	Win
MS13-009 Cumulative Security Update for Internet Explorer 9 for Windows 7 x64 (KB2792100)	EIGHT	Microsoft Corp.	Win
MS13-010 Security Update for Internet Explorer 8 for Windows 7 x64 (KB2797052)	EIGHT	Microsoft Corp.	Win
MS13-010 Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 x64 (KB2789644)	EIGHT	Microsoft Corp.	Win
MS13-010 Security Update for Internet Explorer 9 for Windows 7 x64 (KB2797052)	EIGHT	Microsoft Corp.	Win
MS13-015 Security Update for Microsoft .NET Framework 4 on XP, Vista, Win7, 2008, 2008 R2 x64 (KB2789642)	EIGHT	Microsoft Corp.	Win
MS13-015 Security Update for Microsoft .NET Framework 4.5 on Windows 7, Vista, Win 2008, Win 2008 R2 for x64 (KB2789648)	EIGHT	Microsoft Corp.	Win
MS13-017 Security Update for Windows 7 x64 (KB2799494)	EIGHT	Microsoft Corp.	Win
MS13-018 Security Update for Windows 7 x64 (KB2778344)	EIGHT	Microsoft Corp.	Win

The available patches can be selected and installed, individually or en masse, from the Patch Manager. We found this to be a very simple but effective means of keeping software up to date.

Although there is a separate menu in the program window for licence management, we could not find a means of showing when our licence expired, only how many valid licences we had.

### Client/server antivirus tasks

Scans, both one-off and scheduled, can be set in the Tasks tab.

A vulnerability scan is not required as the Patch Manager constantly monitors software for available patches.

Updating both signatures and the software itself can be carried out from the Clients tab, by selecting the relevant computer(s) and right-clicking. This method can also be used to install or uninstall software.

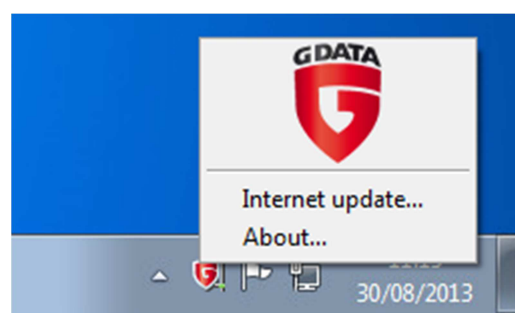
Real-time protection can be enabled/disabled from the Monitor section of the Client Settings tab, as can real-time exclusions.

Scan exclusions can be set in the General section.

USB device control is not available in the software version that we tested.

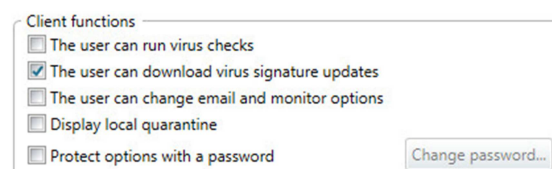
### Client antivirus software

By default, the G Data Security Client has a very minimalist interface. There is a System Tray icon, right-clicking which produces the following context menu:

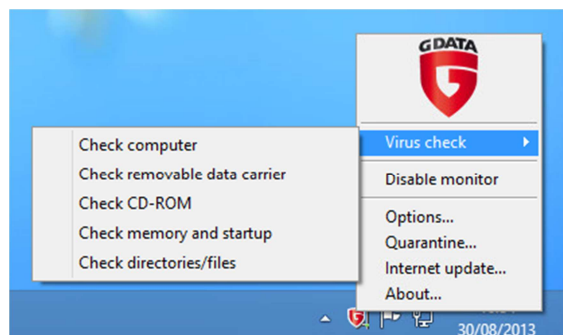


Clicking Internet Update allows the user to update the signatures, and to choose between getting updates from the management server or G Data's Internet servers – for the benefit of mobile users. Other than displaying version information, no other functions are available to the user.

The administrator can optionally hide the G Data icon completely, or allow the users access to additional features:



With all options enabled, the context menu is extended:



of making important information and tasks easy to find. The option of a minimalist user interface for the client software may well appeal to many administrators. Documentation is very good.

If the user is allowed to change email and monitor options, the real-time protection can be disabled; however, this can be password protected, so that only users authorised by the administrator are able to do this.

We note that when real-time protection is switched off, there is only a muted warning from Windows Action Center, i.e. the System Tray icon does not change, and there is no notification shown. Only if the Action Center window is opened is it obvious that virus protection is turned off. However, the G Data system tray does display a warning symbol:



When we attempted to download the EICAR test file, the download was blocked, and the following alert shown in the browser window:



We feel this makes reasonably clear that no further action is necessary.

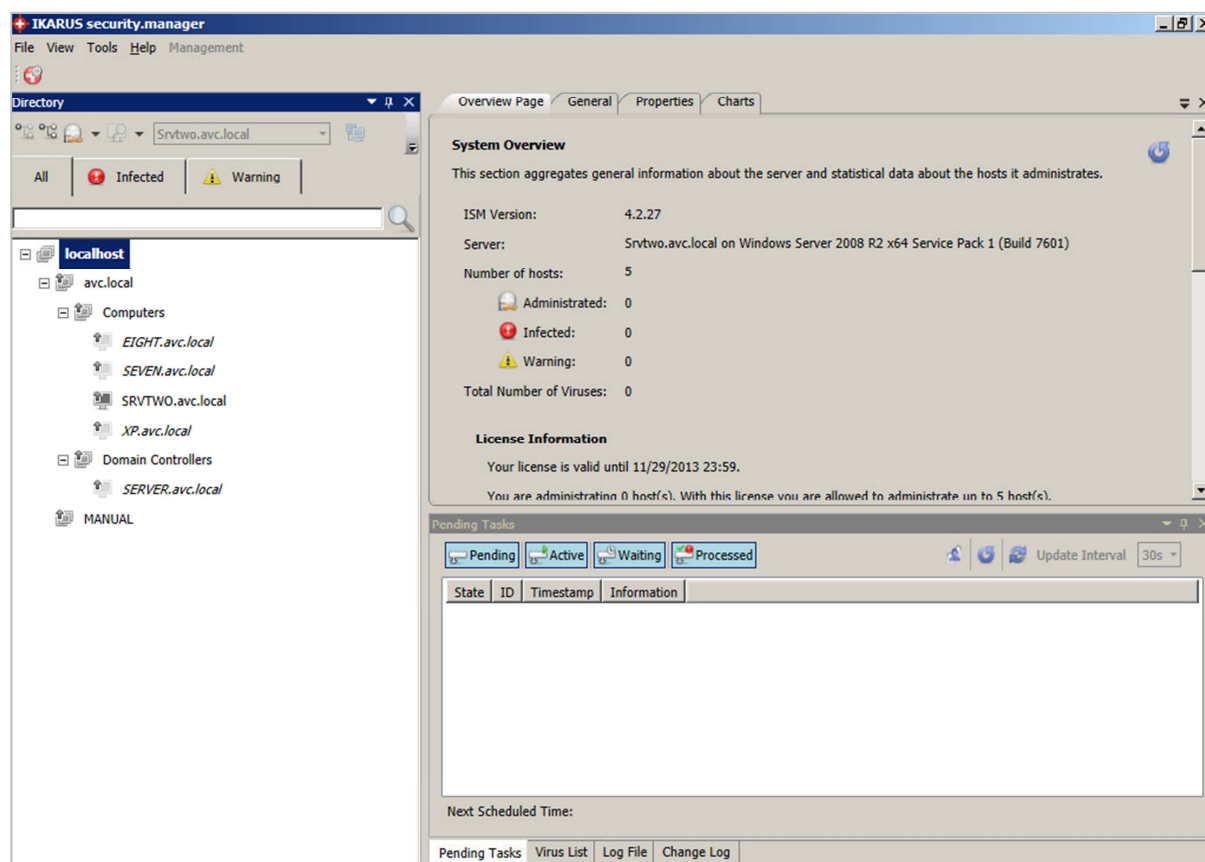
### Server antivirus software

The antivirus software for the server can be considered identical to that for the client.

### Summary

G Data AntiVirus Business with Patch Management impressed us in many ways. Deployment is extremely simple, and the clearly designed console does a very good job

## IKARUS security.manager



### Introduction

IKARUS produce endpoint protection and gateway protection products plus mail and web cloud-security services. For our review, we tested IKARUS anti.virus endpoint protection software, managed by the IKARUS security.manager console.

### Software version reviewed

IKARUS security.manager 4.2

IKARUS anti.virus 2.2

### System requirements

Both the console and the endpoint protection software can be installed on 32 and 64-bit versions of Windows XP, Vista, Windows 7, plus Windows Server 2003, 2008, and 2008 R2. The antivirus software can also be installed on 32 or 64-bit Windows 8. At the time of testing, the IKARUS website did not show Windows Server 2012 as being


supported, so we installed security.manager under Windows Server 2008 R2.

### Downloading the software

Both components of the console (server/client software and user interface) and the accompanying manual can be downloaded from the relevant page of the download section of the IKARUS website.

**Download IKARUS security.manager**

Please download the IKARUS security.manager installation files below.



File	Size
Setup-ISM(server)_v4.2.27.exe	approx. 11,1 MB
Setup-ISM(UI)_v4.2.27.exe	approx. 32,6 MB
ISM user manual	approx. 4,5 MB

## Documentation

IKARUS produce two manuals relevant to this test, one for the console, and one for the client antivirus software. Both are comprehensive, covering all relevant areas of their respective products. The instructions are essentially clear, although both documents show signs of having been imperfectly translated from German; the contents page of the console manual is still entitled “Inhalt”, for example. Both manuals are well illustrated with screenshots. Sadly, neither is bookmarked, although the console guide does have a clickable contents page.

We used the security.manager manual to assist with installing the console and deploying the software.

## Installing the console

The console is installed in two parts, the server software and the user interface. The user interface can be installed on other computers, as well as or instead of the server. Installing the server software requires selecting a language, accepting a licence agreement, manually creating a shared folder, and choosing an SQL installation. If none is available, the setup wizard can install SQL Express 2005 or 2008 automatically. We chose the 2008 variant, which was installed for us without any problems.

The user interface also requires an additional component, in this case the .NET Framework 4; this was also installed automatically by the wizard. We found installing the console to be a very straightforward process.

## Client/server antivirus management interface

The security.manager console has a narrow left-hand column showing the computers on the network; this has tabs to show only infected PCs, or those with a warning. There are also two horizontal right-hand panes. The larger of these shows the details of either the group or individual computer (depending on the view). Tabs at the top allow the view to

be changed to General (a table of important system information for all PCs), Properties (a small selection of configuration items), and Charts (availability, administration and infection of clients, shown as pie charts). We found the General tab to be the most useful, and wonder why this is not the default when the console opens:

localhost

Number of hosts: 5  
Total Number of Viruses: 0  
Number of hosts online: 3  
Number of Hosts Guarded: 1  
Administrated: 1

Hosts	Name	Infections	Online	Service Installed	Administrated	Last Update	Last Time Online
SERVER	SERVER.avc.local	0	●	●	●	N/A	N/A
XP	XP.avc.local	0	●	●	●	N/A	N/A
SRV TWO	SRVTWO.avc.local	0	●	●	●	9/2/2013 14:38	9/2/2013 15:00
SRV ONE	SRVONE.avc.local	0	●	●	●	N/A	N/A
ESDONT	ESDONT.avc.local	0	●	●	●	N/A	N/A

We note that in most views, the main right-hand pane uses the grey colour of the window frame. Whilst the writing on this is definitely legible, we would not describe it as eye-catching. The charts view, on the other hand, uses coloured pie charts on a white background, which we found much more striking.

The lower right-hand pane shows Pending Tasks by default, but can also display Virus List, Log File or Change Log.

## Deploying the antivirus software

Deployment of the antivirus software to clients by push installation could scarcely be simpler. The administrator right clicks on a computer or group, and clicks “Install IKARUS anti.virus”. This applies to server computers as well as clients.

We could not find any alternative method of installing the endpoint software.

## Client/server antivirus monitoring

Whilst the status of real-time protection can be seen for individual computers, by selecting a computer in the left-hand pane and clicking the General tab, there is no means of displaying it for all computers or even a group. An administrator would thus have to click through all computers on the network



one by one to see if real-time protection was enabled. We feel that including RTP in the items displayed for groups/all computers would be a significant improvement.

We also found that the console reacted very slowly to changes in component activation or deactivation, failing to update for over 15 minutes in our test. Closing and re-opening the console immediately updated the display correctly, however. Client status can also be updated manually via the context menu. The date and time of the last update can be seen for groups/all computers under the General tab.

Detailed program information can be seen for each individual computer on the General tab. If malware is discovered on a client, this is shown very clearly in the console. The icon for the computer itself, as well as any groups of which it is a member, turns red with an exclamation mark:



By right-clicking an infected computer and then selecting “Start IKARUS anti.virus”, the administrator can open an exact replica of the program window, exactly as it would appear on the client computer. The title bar indicates the name of the computer whose data is being shown:

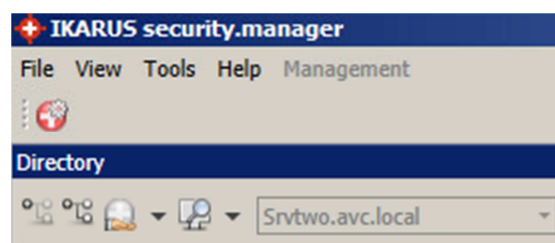


The administrator can then see what has happened with the malware (in this case it can be seen to have been quarantined), and delete or restore files from quarantine, just as if working on the local machine.

Licensing information can be seen on the Overview Page of the console. This shows expiration date of the licence, number of licences purchased, and number being used, which we found helpful.

### Client/server antivirus tasks

The IKARUS security.manager window features a toolbar below the menu bar, which has one single icon, the Configurations button:



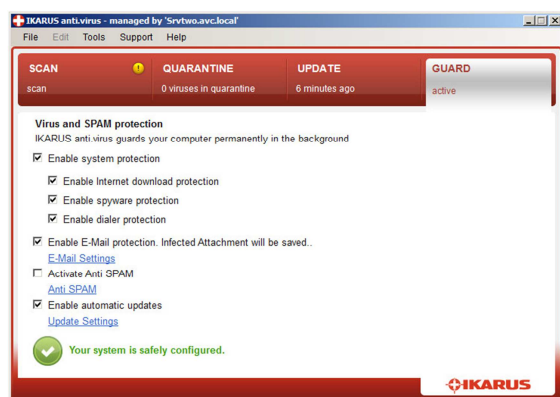
Clicking on this opens the configuration dialog box, which can be used to enable or disable individual protection components, run scheduled scans, set exclusions, and change other settings.

Below the Configurations button is a group of four icons, the rightmost of which can be used to run one-off scans on individual machines (but not on groups of machines). We did not find the other icons in the group very clear, and would suggest that IKARUS could move them to the otherwise virtually empty toolbar and provide them with clear labels.

An individual computer or group of computers can be updated by right-clicking it and selecting “Update IKARUS anti.virus”. Update scheduling can be changed on the Properties page. We could not find any means of updating the program version, controlling USB devices, or scanning for vulnerabilities.

## Client antivirus software

IKARUS anti.virus has a fully featured interface similar to that of a consumer antivirus product. By default, the window opens on the Guard page, which provides a program status display.



Enabling or disabling individual protection features is extremely simple, as these are listed on the page with check boxes. A symbol and text line at the bottom indicate the overall status; “Your system is safely configured” in green with a tick (checkmark) are shown if all is well, but this changes to “Attention! Your system is not safe [sic] configured!” in red with an exclamation mark if the protection components are switched off. A “Fix-All” button is not necessary, given the component display/control on the same page.

In our test, we were able to deactivate the program’s real-time protection using a non-administrator account, without having to enter any additional credentials. However, access can be restricted to specific users/groups, and the administrator can also password protect the client settings.

When we attempted to download the EICAR test file, IKARUS quarantined the file and displayed the following alert:



We feel this makes very clear to the user that malware has been found, but does not indicate what, if anything, needs to be done. If no action is taken, the alert will reappear every few minutes. If the user clicks on SCAN, the program will open on the quarantine page; this recommends that the file should be deleted, and this is easy to do. However, if the user clicks on UPDATE or GUARD, the program opens at the relevant pages, providing no option to deal with the malware found. We feel that many users could be alarmed or confused by this, and may contact technical support; this is not necessary, given that the threat has already been successfully quarantined.

## Server antivirus software

The server antivirus can be regarded as identical to that for the client.

## Summary

We would describe IKARUS’s business software as essentially straightforward and simple to use, but with room for improvement in some areas. The documentation is essentially good but would benefit from bookmarks and tidying up of the English translation. Installation of the console is unproblematic and deployment of the client software particularly quick and easy. We found the management console to be largely simple and effective in its layout, although it could be clarified and tidied up in some areas. Monitoring of real-time protection can only be viewed per machine, and is slow to react.

The main window of the client software is clear and easy to use, and we especially like the ability to reproduce the window of any client on the server, making monitoring and administration of individual PCs very simple. However, we are concerned that malware alerts may cause alarm and confusion with users, and suggest that IKARUS could improve this.

## Kaspersky Endpoint Security for Business Advanced



### Introduction

The Kaspersky Endpoint Security for Business range comprises three different packages: Core, Select and Advanced. We tested the Advanced package for our review, which includes endpoint protection for clients and file servers and vulnerability scanning/patch management. The suite also contains mobile device security and management features, and asset management, patch and vulnerability management, disk/file encryption, OS deployment, and network admission control features.

### Software version reviewed

Kaspersky Security Center 10.0

Kaspersky Endpoint Security for Windows 10.1

### System requirements

Both the console and the endpoint protection software can be installed on Windows XP, Vista, 7 and 8, plus Windows Server 2003, 2008, 2008 R2 and 2012, including Small

Business Server variants. 32 and 64-bit architectures are supported, with one exception: only the 32-bit version of Windows XP is supported for the endpoint software.

Please note that 100 GB free disk space is needed for the patch management feature.

### Downloading the software

We found some confusion on the downloads page of Kaspersky Endpoint Security. There is a separate link for Kaspersky Anti-Virus for Windows Server, but it leads to exactly the same page/download as the link for Kaspersky Endpoint Security for Windows. We feel this could cause confusion and waste time. There are also two versions of the Security Center software available, Full and Lite, but no word of explanation as to what the difference is (the latter includes the client software). Again, we feel this could cause frustration, and suggest that a little more explanation of what is what would make it easier to



download the right software. Kaspersky Lab inform us that steps are being taken to rectify this.

## Documentation

There are no less than four manuals for Kaspersky Security Center. Unfortunately, we did not find the names very helpful in discerning the content of each one, and as noted last year, there are no details given on the website:

Kaspersky Security Center		
Kaspersky Security Center 10		
Administrator Guide For Version 10	English	<a href="#">Download</a>
Getting Started For Version 10	English	<a href="#">Download</a>
Implementation Guide For Version 10	English	<a href="#">Download</a>
User Guide For Version 10	English	<a href="#">Download</a>

We consequently still feel it is rather difficult to find the right manual for the job. The Implementation Guide is in fact the most useful document to help with installation and deployment. It is comprehensive at 92 pages, clear, well bookmarked and has a clickable contents page, making navigation easy. As with last year's version, there are no screenshots at all, which we feel is a shame.

## Installing the console

The setup wizard involves accepting a licence agreement, choosing typical or custom installation (we chose typical), and specifying the number of computers to be protected, in groups ranging from less than 100 to over 5,000. A progress display shows the required components, which of these are already there, which have to be installed; in our case, we needed SQL Server 2008 R2 Express SP2 and MSXML 4.0, but these were installed automatically by the wizard.



After completion, the Quick Start Wizard runs. This requires the administrator to enter the licence key to activate the products, and allows some settings such as proxy server to be changed. Finally, the option is provided of starting the deployment wizard.

## Client/server antivirus management interface

Kaspersky Lab's administration console uses the familiar Microsoft Management Console (MMC) framework. This consists of a narrow left-hand pane with various options, and a much wider right-hand pane to display the chosen option. It opens with the main page of the Administration Server selected. This is divided into 6 sections: Deployment, Computer Management, Protection and Virus Scan, Update, Monitoring, and Administration Server. All but the last of these have their own status displays, in the form of a "traffic light" button, showing green, amber or red for problem/warning/safe states respectively. Each section has links to relevant tasks, e.g. the Deployment section has a link entitled "Install Kaspersky Anti-Virus". This page provides a simple, at-a-glance overview of the state of the network, with easy access to any important tasks that need doing.

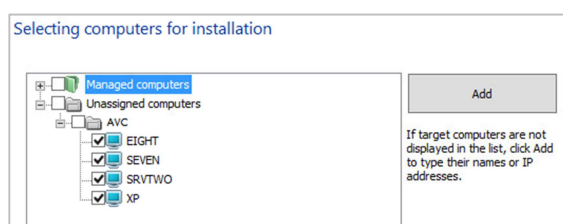
The left-hand pane of the window, consistent with Windows, contains a folder tree with more detailed options. These include Managed Computers (displays status and allows everyday management), Reports and Notifications (protection, deployment and

update status as pie charts), Applications and Vulnerabilities (application control and update monitoring), Remote Installation, and Repositories (management of installation packages, updates and licences).

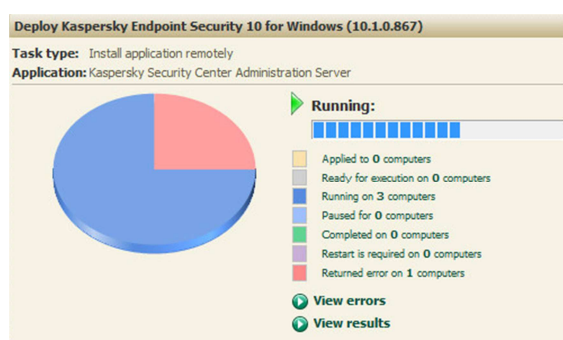
Kaspersky Security Center makes a wide variety of views and tasks available, but we feel the use of the familiar MMC console and good graphical design nonetheless make it very straightforward to find one's way around.

### Deploying the antivirus software

Deployment to clients by push installation uses the Remote Installation Wizard. If the full Kaspersky Security Center has been downloaded, the client endpoint software is already integrated, so the administrator only has to select the computers for deployment:



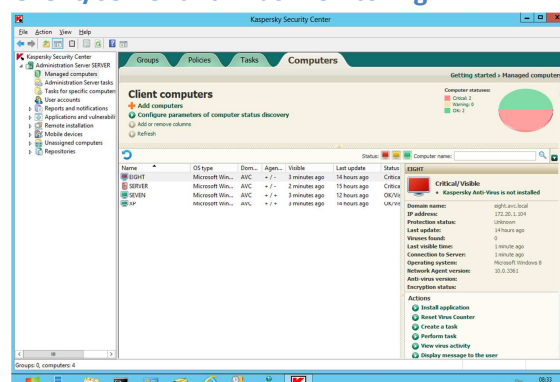
The wizard asks whether client PCs should be restarted automatically, not at all, or after a warning to users. Installation then proceeds, and a very clear pie chart shows the progress in real time:



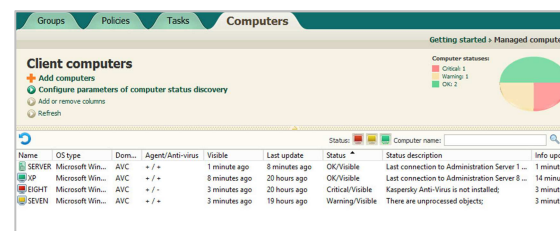
Kaspersky Endpoint Security software can be installed on the server in the same way and at the same time as on the clients. It is automatically configured slightly differently from the clients, but deployment is identical.

We found the remote push installation to be very quick and simple.

### Client/server antivirus monitoring



The overall status of real-time protection can be seen on the Statistics tab of Reports and Notifications as a pie chart. We note that a warning is only shown in the event that all the protection components are deactivated. The status of individual PCs is shown in the Computers tab of Managed Computers, with a traffic-light colour scheme:



The time of last update, database signature version, program version and number of malware detections can also be seen on the Computers tab of Managed Computers.

We could not find a means of monitoring the status of Kaspersky Lab's firewall on the client.

Outdated software is displayed in Application Vulnerabilities, a sub-item of Applications and Vulnerabilities.

Licensing information can be found in Repositories/Keys.

### Client/server antivirus tasks

Malware scans, vulnerability scans and updates can be run by right-clicking a computer or group and selecting All Tasks/Create a Task from the context menu.

The program version can be updated by rerunning the deployment wizard.

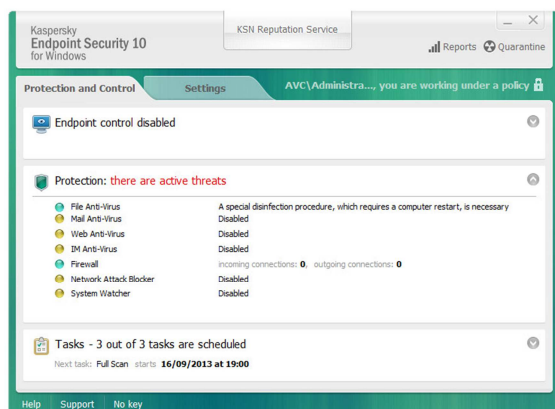
Components such as real-time protection or firewall can be enabled or disabled by policy, under Managed Computers/Policies.

It is not possible to uninstall individual components such as the firewall. Kaspersky Lab informs us that this is due to the close integration of the protection components with each other.

We could not find out how to set scanning exclusions or control USB devices from the console, despite searching the Implementation Guide and Knowledge Base. We suggest that Kaspersky Lab should provide better documentation on how to access and configure these features.

### Client antivirus software

Kaspersky Endpoint Security's program interface is quite different from that of any of the other programs in this review. It provides the administrator with detailed information about the status of individual components and settings, but by default does not allow any actions to be carried out or the configuration to be changed.



From the point of view of standard users, we would regard the interface as “minimalist”, in the sense that they are not supposed to interact with it. Administrators could however enable some functionality, such as carrying out updates and scans, from the console.

By default, it is not possible to disable real-time protection from the program window, regardless of the type of Windows account being used.

By default, detected malware is blocked silently, but this can be configured by the administrator.

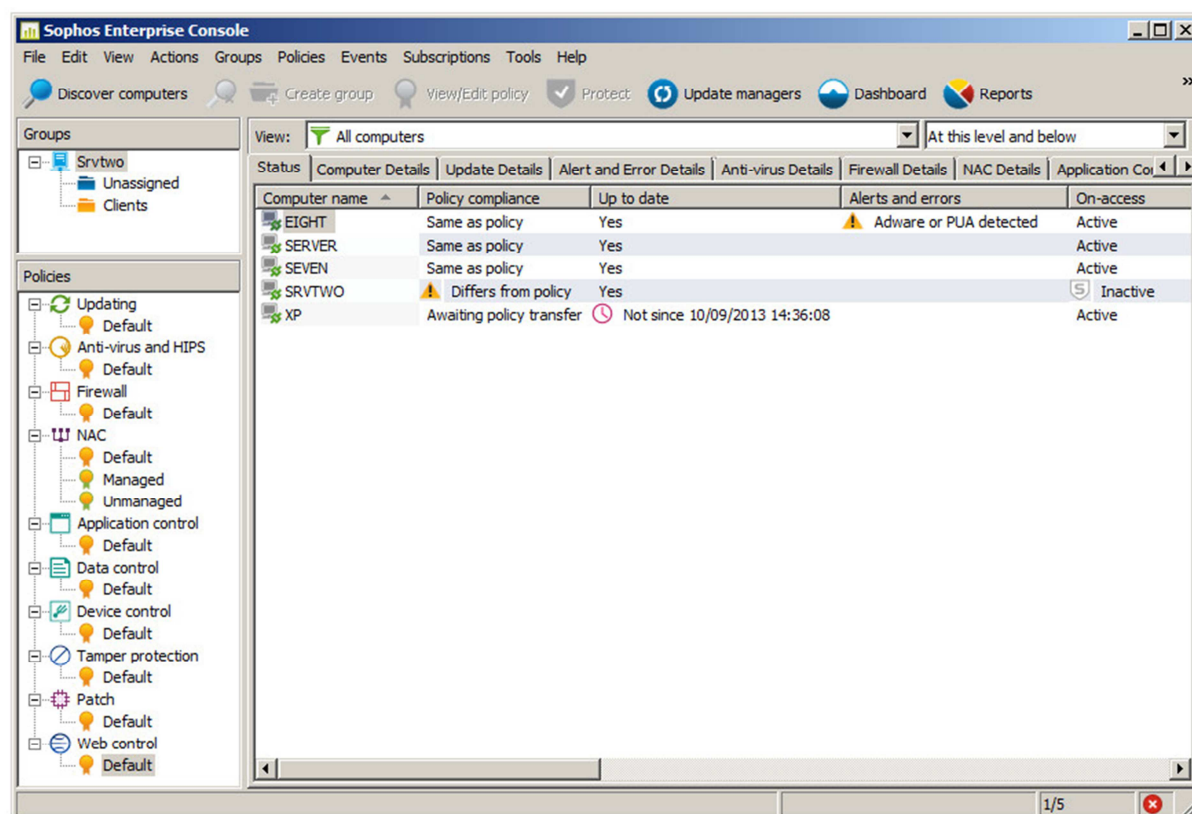
### Server antivirus software

The same software as for the clients is installed on the server, although it is configured differently by the setup wizard. For example, the Endpoint Control feature is not installed, and so this section is not displayed in the main program window. Otherwise, the interface of the server software is identical to that of the client.

### Summary

Kaspersky Lab's console is very powerful, but the use of the familiar mmc format means that administrators will easily find their way around the interface. The graphic design and use of e.g. pie charts to show deployment progress add to the user-friendliness. By default, the client software is minimalist from the point of view of the user, but provides the administrator with useful status information. Documentation is also good, once the right manual has been found. Our once concern is that it is very difficult to find exclusion and USB-device control settings.

## Sophos Endpoint Security and Control



### Introduction

Sophos specialise in security software for business and provide a wide range of products and services. For our review, we tested the Endpoint Security and Control client software, managed by the Sophos Enterprise Console.

### Software version reviewed

Sophos Endpoint Security and Control 10.2  
 Sophos Enterprise Console 5.2

### System requirements

Sophos Endpoint Security and Control is supported for Windows XP, Vista, 7 and 8, in 32 and 64-bit architectures; also for Windows Server 2003, 2008, 2008 R2, 2012, and Small Business Server versions of these, in 32 and 64-bit architectures where applicable. To simplify the installation of SQL Server, we tested the suite on Windows Server 2008 R2 64-bit.

### Downloading the software

Sophos provided us with a direct link to download the software. Documentation can easily be found in the Support section of the Sophos website.

### Documentation

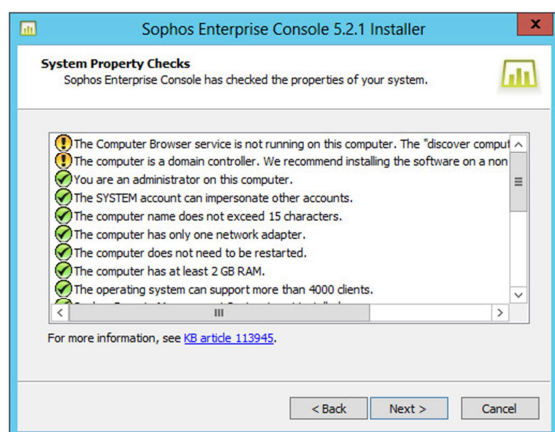
To assist with the installation and deployment, we used the Sophos Enterprise Console Quick Startup Guide. This is relatively brief at 29 pages, though in some areas there are links to pages of the Sophos online knowledge base, which provide additional information. If the external knowledge base pages are included, the manual provides everything the administrator needs to know to install the console and deploy the client software. It is clearly laid out and well written, although there are unfortunately no screenshots at all. There is a clickable contents page and the document has been

well bookmarked, so it is easy to get to a particular page or section.

Other documentation is available, including a 57-page advanced startup guide, and a 123-page Help guide.

### Installing the console

The first step of installation is unpacking the setup software. This involves agreeing a licence agreement and selecting which components to install (the interface can be installed on additional computers for ease of access). The wizard provides a list of requirements and shows which of these have been fulfilled, which we found very helpful:



The actual installation process which then follows is straightforward; it requires the administrator to have created Sophos-specific user accounts in advance, but this is explained in the manual. An SQL Server installation is also required; the 2008 Express version can be installed automatically if desired, and we chose this option.

### Client/server antivirus management interface

The main pane of the console window shows either all managed computers or those in a specific group – this can be selected in the upper right-hand pane. Tabs along the top of the main pane allow different information to be shown in different views, including Status (= protection, the default view), Computer Details (OS, Service Pack, IP address, current user etc.), Update Details, Anti-virus Details,

and status of various other protection components. A very wide variety of information can thus be seen simply by clicking through the tabs at the top.

The lower pane on the left-hand side shows the various configuration policies; right-clicking any of these allows the policy to be edited. The console also has a menu bar and toolbar.

Given that a considerable amount of information can be displayed, we found the layout of the Sophos Enterprise Console to be very straightforward.

### Deploying the antivirus software

The “Download Security Software Wizard” launches when the console is opened, and takes the administrator through the installation process. It asks for the client types to be protected – we note that older versions of Windows are still supported:



Next, computer groups have to be created; these can be imported from Active Directory, which we found very convenient. The administrator then right-clicks a group, and selects Protect Computers from the context menu. Servers can be installed along with clients, there is no need to run the process again. We found the deployment process to be very simple and unproblematic. The client software can also be installed manually on individual computers.

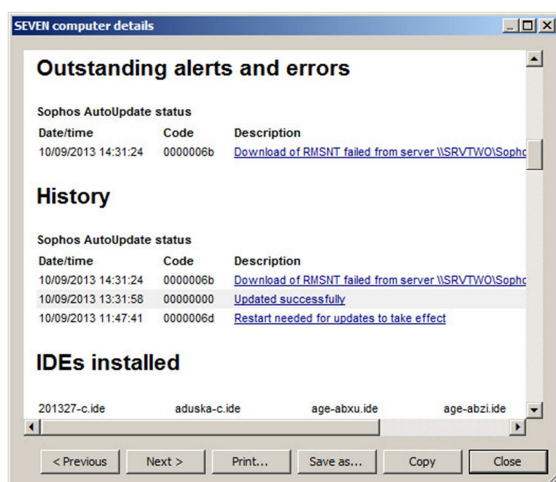


### Client/server antivirus monitoring

Amongst other things, the Status tab of the console shows whether signatures are up to date, if real-time protection is enabled, and the state of the Sophos firewall (if installed). We noticed that the status display responds very quickly (just a few seconds) when e.g. a computer is shut down or a protection components switched off.

The program version and virus signature database details can be seen under the Anti-virus details. Malware detections are shown on both the Status tab and Alert and Error Details tab.

Double-clicking a computer from any view tab will open up a detailed report on that machine. We were impressed to see that in the event of an error (e.g. update failure), the report contains a hyperlink to a page on the Sophos website with potential causes of and solutions to the problem. In the case of a malware discovery, there is a similar link to the Sophos website, which will provide details of the malware concerned.



Vulnerabilities can be seen under the Patch Details tab of the main pane.

The console has a Subscriptions menu, which makes it easy to access detailed licensing information.

### Client/server antivirus tasks

Updates and full scans can be carried out by right-clicking the computer group in the top-left pane, or one or more computers selected in the main pane; the commands Update Computers Now and Full System Scan are available on the context menu.

Scheduled scans and exceptions for these can be configured using the policy dialog for the Anti-virus and HIPS component.

Vulnerability scans (patch assessments) are run automatically according to a schedule defined in the relevant policy.

The automatic schedule can be changed by double-clicking the icon for the default updating policy in the lower-left pane of the console window.

We could not find a means of updating the program version, other than re-running the deployment wizard.

To enable or disable individual components such as the real-time protection or firewall, an appropriate policy can be created and assigned to the relevant clients. This is done by right-clicking the policy icon for the component concerned and selecting Create Policy.

Protection components such as the firewall can be added or removed by re-running the deployment wizard (right-click a computer or group and click Protect Computers). This provides a component choice page, from which any item can be added or removed.

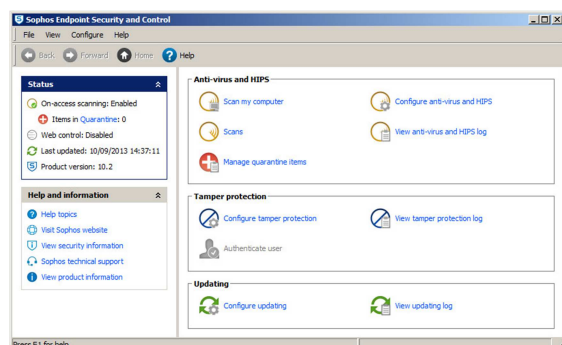
Device control is carried out using the policy of the same name.

### Client antivirus software

The Sophos Endpoint Protection and Control software has a fully featured client interface, not unlike that of a consumer security

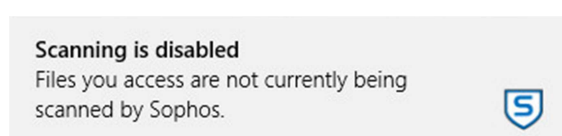


product. It is reminiscent of the Windows XP Explorer:



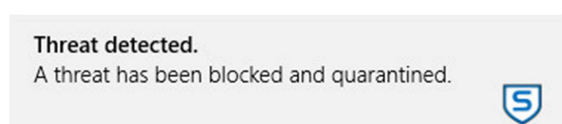
Scanning functionality is provided on the home page of the program: Scan My Computer runs a full scan, whilst Scans allows a custom scan to be run. There is no update button or menu item in the window, but right-clicking the system tray icon allows an update to be run.

The Status panel, in the top left-hand corner of the window, shows the status of real-time protection and updates. When we disabled real-time protection, there was no obvious warning in the window, although Sophos displayed a Windows 8 warning message (or System Tray message in earlier versions of Windows):



The same alert is shown when logging on to the computer. When logged on with a standard user account, we were not able to deactivate real-time protection, as the controls were greyed out.

When we attempted to download the EICAR test file, Sophos blocked the webpage and displayed the following alert:



We feel this makes clear that no further action is necessary.

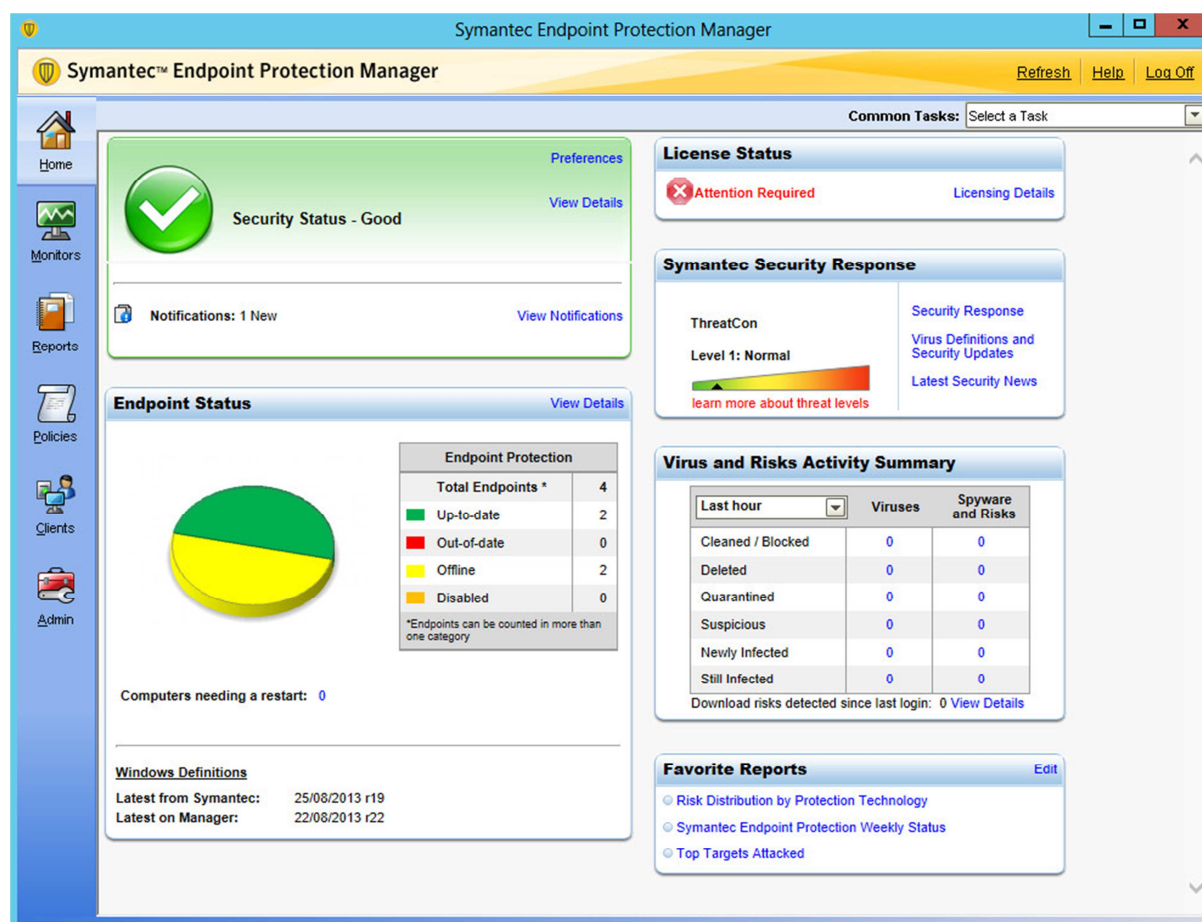
### Server antivirus software

The interface of the server antivirus software can be considered identical to that for the clients.

### Summary

We found installing the Sophos console and deploying the client software to be unproblematic, with assistance from the Quick Startup Guide. Despite housing a wide range of functions, the console is straightforward to navigate. The client software is also clear and provides standard functionality. We feel that experienced IT professionals will feel entirely comfortable with the Sophos software, and that with minimal training it could be used by non-expert administrators too.

## Symantec Endpoint Protection



### Introduction

Symantec make a wide range of security products for businesses large and small. Endpoint Protection uses a locally installed management console to deploy and manage endpoint protection software for client PCs and file servers.

### Software version reviewed

Symantec Endpoint Protection Manager 12.1  
Symantec Endpoint Protection 12.1

### System requirements

Client operating systems: Windows XP, 32-bit; Windows Vista, 7, 8, in both 32 and 64-bit architectures.

Server operating systems: Windows Server 2003, 2008, 2008 R2, 2012, including all

Small Business Server variants, all 32 and 64-bit.

### Downloading the software

Having completed the registration for the trial version, the user is taken to the download page. There are two items available in English (software and tools), both clearly marked and easy to find. When run, the main .exe file extracts not only the setup files but also the documentation, which we find very convenient.

### Documentation

The documentation included in the downloaded package consists of a 132-page guide to the client software, a 28-page Getting Started guide, and a comprehensive 1,156 Installation and Administration Guide. All three are well organised and written, and

extensively bookmarked, but unfortunately completely lacking in screenshots. The Getting Started guide only covers client deployment using a link in an email, so we used the Installation and Administration Guide to assist us in deploying the client software.

### Installing the console

This is a very simple process, involving accepting the licence agreement, choosing the installation folder, and stating whether more or less than 100 clients will be protected. At the end of the process, a message box states that a database is being created and initialised, and that this “will take a few minutes”; this actually turned out to be 25 minutes, at the end of which we had started to wonder whether the process had hung.

### Client/server antivirus management interface

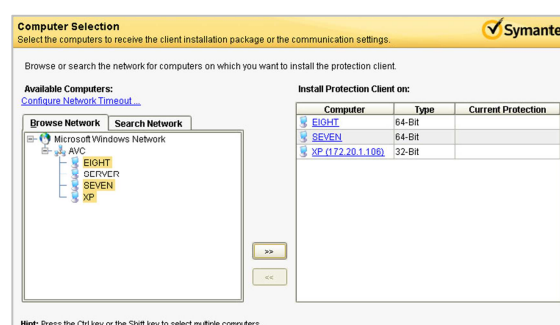
The Home page of Symantec Endpoint Protection Manager features boxes for overall and individual security status, license status and recent malware events. We feel this provides the administrator with a good overview of the state of the network and would highlight any problems immediately. A left-hand menu column provides links to Monitors, Reports, Policies, Clients and Admin. Monitors provides access to logs and other statistics; Reports enables the administrator to display highly customised information summaries; Policies allows specific client configuration to be applied to groups of client PCs; Clients displays a list of all the individual PCs on the network and allows a variety of monitoring and administration tasks to be carried out. Admin enables configuration of console users. We feel the layout of the console is clear and simple and enables the administrator to find relevant areas quickly and easily.

### Deploying the antivirus software

When the console is first opened, a welcome dialog is displayed:



The Client Deployment Wizard can also be started from the Common Tasks list in the console. Remote push installation requires an installation package and options to be selected from a single dialog box; the computers to be installed are then selected from a list:



Once installation has started, a real-time status report is provided. The client PCs have to be restarted after the software has been installed. There is no choice of components (such as the Symantec firewall) available during the installation process. However, a custom installation package can be made, allowing administrators to select or deselect whichever components they want.

We found deployment using remote push to be very quick and straightforward.

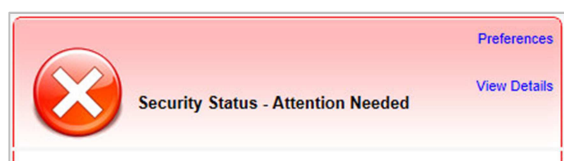
We installed the file server protection in exactly the same way as the client software. The process has to be run again for servers as

the software configuration for them is different.

There are two alternative installation methods for client PCs. The administrator can email users with a hyperlink to the client software. The user installing the software needs administrator credentials to carry out the procedure. Alternatively, an executable installation package can be saved to a file share on the server, so that the user or administrator can browse to the network share from the client PC.

### Client/server antivirus monitoring

The Security Status box in the top left-hand corner of the console window shows the state of important protection components, such as real-time protection and firewall. If all is well, the box is green and displays the text "Security Status – Good". In the event of a problem, even with a single client PC, the box turns red and warns "Attention Needed":



Clicking on View Details displays a comprehensive list of protection components, with any that are disabled marked in red; the hostname and IP address of all affected PCs are given.

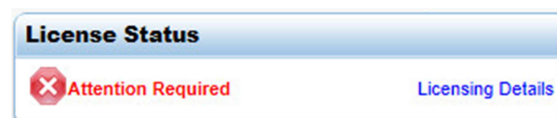
The Endpoint Status box below Security Status shows how many PCs have up-to-date signatures, and how many are out of date; clicking on View Details opens a list of all the PCs on the network, showing OS, logged-on user, IP address, time of last scan, date and version of signatures, and status of individual protection components.

The version of the endpoint software installed can be found by clicking the Clients tab in the vertical menu column at the left-hand edge of the window.

Malware discovered is clearly displayed in the Virus and Risks Activity Summary box on the Home page of the console. It is divided into two categories, Virus and Spyware/Risks, and the time period to be shown can be set to anything between an hour and a year.

We could not find any means of scanning for vulnerabilities.

Licensing information is shown in the License Status box in the top right-hand corner of the console window. This displays a warning in the event of a problem:



Clicking on Licensing Details opens a detailed information page; although this claims to provide licence expiration dates, this was the one bit of licensing information we were unable to find.

### Client/server antivirus tasks

A variety of tasks can be run from the Clients view of the console, including scans and updates:

Name	Health State	Logon User or Computer	IP Address	Client Version
Eight	Online	Administrator	172.20.1.104	12.1.3001.165
Server	Online	Administrator	172.20.1.200	12.1.3001.165
Server	Online	Administrator	172.20.1.105	12.1.3001.165

Delete	Switch to Computer Mode	Scan Update Content Update Content and Scan Restart Client Computers Enable Auto-Protect Enable Network Threat Protection Disable Network Threat Protection Enable Download Insight Disable Download Insight
Move		
Run Command on Computers		
Edit Properties		

Running the scan command opens a dialog box with a choice of quick, full or custom scans. The same context menu also allows individual protection components to be enabled or disabled, though it does not allow real-time protection to be deactivated. A command to restart the selected computer(s) is also available.

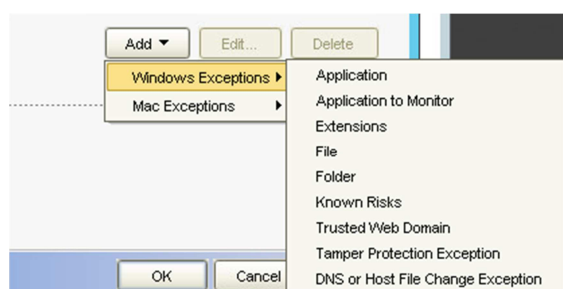
A policy is used to schedule scanning of client PCs. The console allows the default scan to be edited, or new scans to be created.

Automated updates are also controlled by a policy. By default, this checks for new updates every four hours. The policy can easily be altered to make updates more or less frequent.

Components of the suite can be added or removed by rerunning the Client Deployment Wizard, and deploying a customised installation package. This worked very well in our test; the endpoint protection software on the client was stopped and then immediately restarted with the new configuration.

Rerunning the deployment process could also be used to update the version of the endpoint protection software.

Excluding a specific file or folder from scanning can be done by going to Policies and clicking Exceptions. This allows a wide variety of items, including applications and web domains, to be excluded from scanning:



Symantec Endpoint Protection Manager can block devices such as USB flash drives. This can be done by going to Policies, selecting Application and Device Control, editing the default policy, and adding the appropriate device type to the Device Control list. We found this very intuitive, and once we had clicked "Assign the policy", the USB flash drive plugged into one of our client PCs was almost immediately rendered invisible in Windows Explorer. The administrator can

choose to display a message on the client PC when the device is blocked.

### Client antivirus software

The client software of Symantec Endpoint Protection has a similar interface to consumer antivirus products:

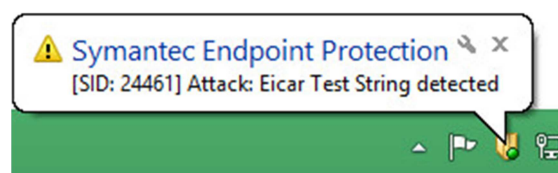


There is a big and obvious status display at the top of the window. This uses text, an icon and colour to show whether all is well. In the event of a problem, a "Fix All" button appears in the status area; clicking this reactivates any disabled components.

Using the items in the menu column on the left, the user can update signatures, and run either a quick scan or a full system scan.

When logged on to the PC with a non-administrator account, the menu items for disabling protection components are all greyed out and thus cannot be used.

When we attempted to download the EICAR test file, Symantec Endpoint Protection blocked the download and briefly displayed the following message:



As the message disappears after only 4 seconds, and does not link to any further

information, we are not convinced of its value.

### Server antivirus software

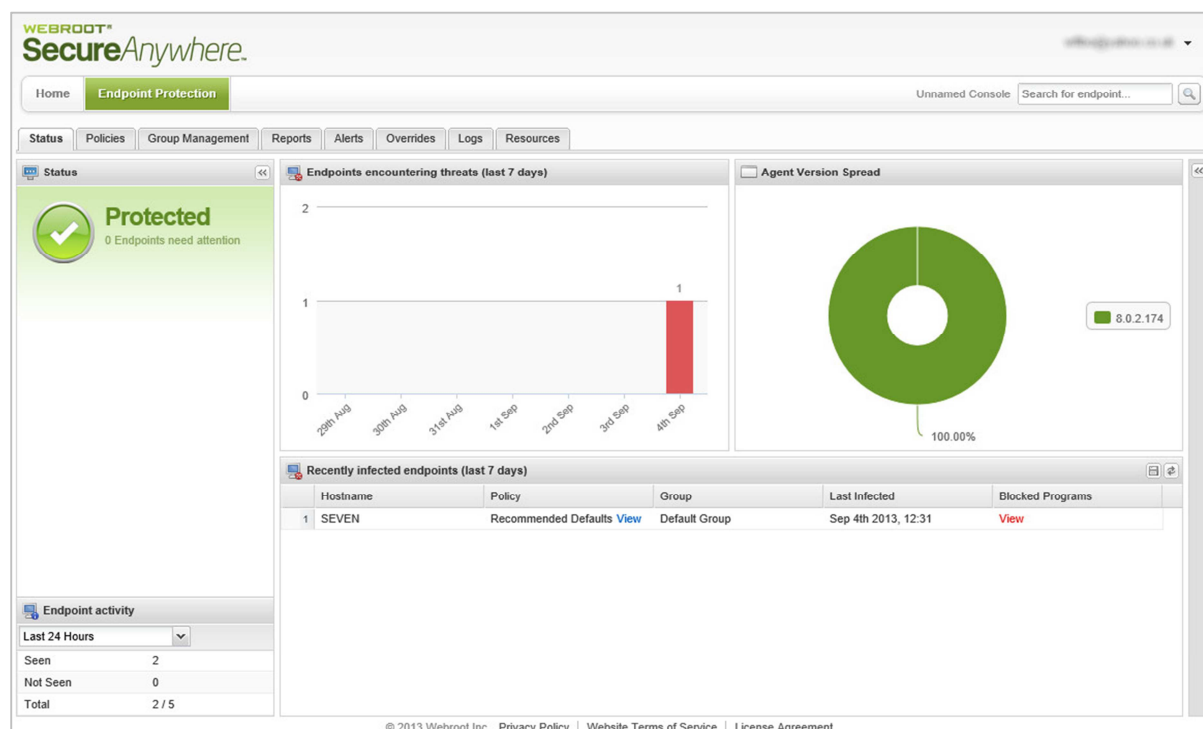
The server antivirus software can be regarded as identical to the client software in terms of interface. The deployment wizard provides the option of installing only "Basic" protection (without firewall), which we took. Only the Virus and Spyware Protection strip is then shown in the program window.

### Summary

We found protecting our network with Symantec Endpoint Security to be very convenient and trouble-free. The management console has been graphically well designed, displaying important information without overwhelming the user, and making everyday tasks easy to find and carry out. The software was very reliable and unproblematic in our test. We feel it should prove very easy for IT professionals to use, and only minimal training would be required for non-expert administrators.



## Webroot SecureAnywhere Endpoint Protection



### Introduction

Webroot's business security software uses a cloud-based console to manage endpoint security software on client and server computers.

### Software version reviewed

Webroot SecureAnywhere Endpoint Protection 8.0

Webroot SecureAnywhere Console as at 4<sup>th</sup> September 2014.

### System requirements

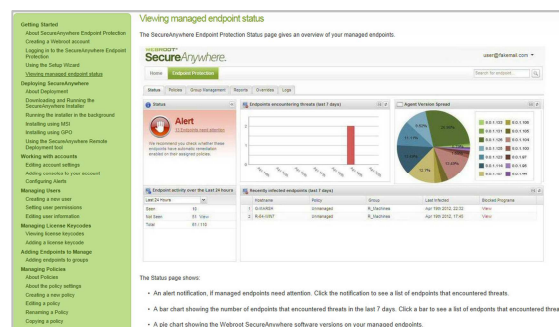
Webroot SecureAnywhere Endpoint Protection runs on Windows Server 2003, 2008, 2008 R2, and 2012, all in 32 and 64-bit versions where applicable. Supported Windows client operating systems are Windows XP, Vista, 7 and 8, again all in 32 and 64-bit versions. Additionally, Mac OS® X v.10.7 "Lion" and Mac OS X v.10.8 "Mountain Lion" are supported.

### Downloading the software

This is not applicable, as the console is web-based.

### Documentation

Webroot provide a comprehensive online help service, which could be described as an online manual. It covers all aspects of using the software, starting with creating a Webroot account. It is easy to navigate, due to a contents panel on the left-hand side of the page, and is illustrated with screenshots where necessary:



A searchable online FAQ page is also available.

### Installing the console

This is not applicable, as the console is web-based.

### Client/server antivirus management interface

Logging on to the SecureAnywhere console involves entering two characters of a “Personal Security Code”, a word or number at least six characters long, created when the Webroot account is set up.

The Home page of the console simply has links to the Endpoint Protection page and Webroot Community. We would regard the Endpoint Protection page, shown in the main screenshot above, as the main status display. It is made up of four main panels: Status; Endpoints Encountering Threats; Agent Version Spread (program version); and Recently Infected Endpoints. A row of tabs along the top of the console provides access to various tasks and information, including Policies (client configuration), Group Management (everyday administration tasks), Logs, and Resources (installation and deployment area). We found the layout of the console to be clear and straightforward.

### Deploying the antivirus software

Direct installation of the endpoint software from the client is extremely quick and easy. The administrator merely needs to log on to the console, go to the Resources page, click Windows Download, and then Run. No further action is necessary, and the software is installed in seconds. The same method is used for servers as for clients.

### Client/server antivirus monitoring

In our test, the console did not warn in any way when we disabled real-time protection on a client. However, Webroot inform us that program’s entire functionality is contained within the WRSVC service/WRSA.exe, and that if this is switched off or fails to start, the

endpoint protection will be shown as inactive in the console.

Due to the cloud-based nature of the product, there is no information shown about signature versions or time of last update; the client always uses the latest definitions from the cloud.

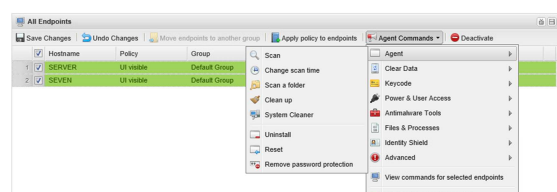
Details of the program version installed can be seen in overview on the Status page, or in detail for each individual client on the Group Management page.

Malware discoveries are shown in the Recently Infected Computers pane of the Status page. We did not find any sort of vulnerability scan in the software.

Licensing information can be displayed by running Agent Version Spread in the Reports section or in the Group View.

### Client/server antivirus tasks

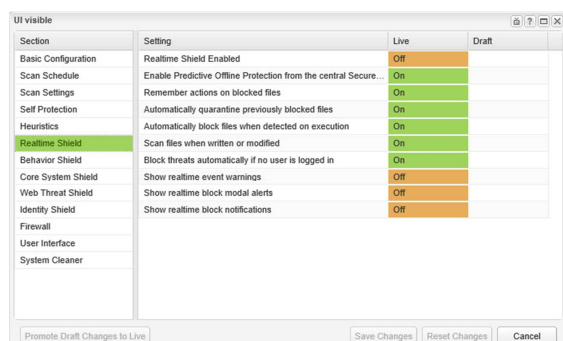
A variety of tasks can be carried out from the Group Management page. Computers can be selected individually or by group, and the Agent Commands menu allows the administrator to scan, change scheduled scan times, or uninstall the software, amongst other things.



Additional commands available include logging off the current user, shutting down or restarting the PC, or even restarting in Safe Mode with Networking, which we found particularly thoughtful – this is very useful in the event of a malware infection.

Updating signatures is not relevant, due to the cloud-based nature of the program.

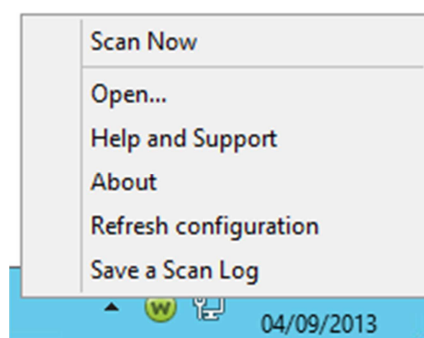
Enabling or disabling individual components can be done via policy. The administrator creates a new policy, which can be altered very easily from the configuration dialog box:



USB devices can be controlled by setting the highest level of heuristics in the policy. Webroot tell us that scan exclusions are not necessary, as all files and processes are already classified by the security software.

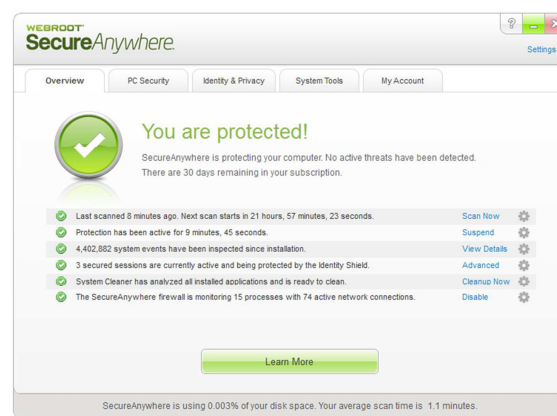
### Client antivirus software

By default, Webroot's client software has a minimalist interface. There is a system tray icon; right-clicking this displays the following context menu:



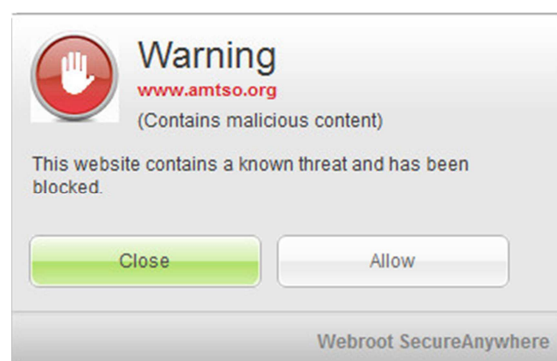
The only action available to the user is to start a pre-configured scan. Clicking "Open..." merely shows a message box, stating that the user should contact the administrator to access the user interface.

It is possible for the administrator to enable the full user interface, which has a program window identical to that of Webroot's consumer antivirus software:



However, most of the controls, including those for enabling or disabling individual components, are disabled; clicking any of them displays a message stating that the program is centrally managed. We feel that most administrators would regard such a program window as being merely a distraction, and that the default minimalist interface makes more sense.

When we attempted to download the EICAR test file, Webroot blocked the download and displayed the following message:



Clicking on Allow displays a further message: "Your administrator has blocked access to this function". We feel that whatever the user clicks, it is clear that the download has been blocked.

### Server antivirus software

The server software and its possible configurations are identical to those for the clients.

### Summary

Webroot SecureAnywhere Endpoint Protection is very straightforward to use. The console is clear, and deployment via individual

installation on client machines could easily be carried out by non-expert administrators. The online help is also good.

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G Data	IKARUS	Kaspersky Lab	Sophos	Symantec	Webroot
Recommended product for:										
up to 5 Clients, Server	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender	ESET Endpoint Security	F-Secure Client Security	G Data SmallBusiness Security	IKARUS security.manager	Kaspersky Small Office Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Cloud	Webroot SecureAnywhere Business - Endpoint Protection
up to 25 Clients and 1 Fileserver			ESET Endpoint Protection Standard		G Data EndpointProtection Business		Kaspersky Business Space Security		Symantec Endpoint Protection Small Business Edition	
up to 25 Clients and Fileserver and Messaging Server		Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Secure Business	F-Secure Business Suite	G Data EndpointProtection Enterprise		Kaspersky Enterprise Space Security	Sophos Endpoint Protection - Advanced	Symantec Protection Suite Enterprise Edition	
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server					G Data EndpointProtection Enterprise plus PatchManagement					
Features Management Server										
What is the maximum number of clients overall?	1000	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	25000	unlimited	unlimited
Master-Slave-Server										
Multiple AV Servers	•		•		•		•		•	
Master server controls slave server in different offices	•		•		•	•	•		•	
Slave server for distributing updates	•	•	•	•	•	•	•		•	
Client installation										
Which client deployment methods does the product support?										
Does the product include a mechanism that allows the administrator to push the software to the clients?	•	•	•	•	•	•	•	•	•	•
Does the product include a mechanism that allows the end user to download and install the software?		•	•	•	•		•	•	•	•
General Capabilities										
Does the product allow administrators to assign different policies to different groups of computers (regardless of the person logged in)?	•	•	•	•	•	•	•	•	•	•
Does the product support static groups (i.e. user or computer are assigned manually to a group or are imported from a third party system)?	•	•	•		•	•	•	•	•	•
Group Import & Synchronisation										
Can changes in Active Directory be synchronized?	•		•			•	•	•	•	•
Can computers/users be imported from other LDAP server?	•		•	•		•	•		•	•
Can computers be imported by a GUI	•		•	•	•	•	•		•	
Can different actions be defined based on the malware category?	•				•	•	•		•	•
Microsoft Exchange										
Exchange 2003 / 2007 / 2010	•	•		•	•	•	•		•	
Network shares										
Can a user or administrator scan network shares after entering a password?	•						•		•	•
Email Messages										
Microsoft Outlook	•	•	•	•	•	•	•		•	
Lotus Notes	•		•		•		•		•	
Thunderbird	•	•	•		•		•			
Archives										
ZIP/RAR/ARJ & archived installers	•	•		•	•	•	•	•	•	
Conditions										
Remediation										
Does the product provide remediation capabilities?		•	•	•	•		•	•	•	•
General capabilities										
Firewall Rules										
Does the product come with default policies for workstations?	•	•		•	•	•	•	•	•	•
Does the product come with default policies for server?		•		•	•	•	•	•	•	•
Client Management										
Client User Interface										
Can the administrator limit or control configuration changes by the end-user?	•	•	•	•	•	•	•	•	•	•
Can different policies be applied for different computers?	•	•	•	•	•	•	•	•	•	•
Depending on the location of the device (i.e. Office, Hotel, Home, etc)	•		•		•	•	•		•	•
Depending on group membership of the computer	•	•	•		•	•	•		•	•
Depending on group membership of the user (i.e. administrator vs. normal user)				•	•	•			•	•
Administrator Management										
Rights / Access Control										
Does the product support multiple administrators and different access levels?	•	•	•	•	•		•	•	•	•
Device Control										
Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?			•	•	•		•	•	•	•
Can you lock										
DVD / USB / external media			•	•	•		•	•	•	•
Floppy			•	•	•		•	•	•	•
other			All ports and all removable media can be locked, but it's possible to add exceptions for any individual ports or media	Any PnP devices	Webcam		Printers, CD/DVD, modems, multifunctional devices, external network adapters, wi-fi, Bluetooth devices		Firewire, Bluetooth, printers, modems, wi-fi, CD/DVD/Bluarray, card readers	
Failover										
What if the AV Server (local) hangs up										
automatic switching to a second local server		•	•		•		•	•	•	
updates from vendor-server instead of local server	•	•	•	•	•	•	•	•	•	
other			Log and notifications	Multiple proxy servers and proxy chaining supported		It is not set by default but you can define that if the server is not responding, the AV should use the IKARUS online server				Local endpoint Agent can always communicate with the cloud, plus local 'offline' policy protects even if communications are lost.





Feature list	Avira	Bitdefender	ESET	F-Secure	G Data	Ikarus	Kaspersky Lab	Sophos	Symantec	Webroot
Recommended product for:										
up to 5 Clients, Server	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender	ESET Endpoint Security	F-Secure Client Security + F-Secure Server Security	G Data SmallBusiness Security	IKARUS anti.virus	Kaspersky Small Office Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Cloud	Webroot SecureAnywhere Business - Enterprise Protection
up to 25 Clients and 1 Fileserver			ESET Endpoint Protection Standard		G Data EndpointProtection Business	IKARUS security.manager	Kaspersky Endpoint Security for Business SELECT	Sophos Endpoint Protection - Advanced	Symantec Endpoint Protection Small Business Edition	
up to 25 Clients and Fileserver and Messaging Server		Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Secure Business	F-Secure Business Suite	G Data EndpointProtection Enterprise		Kaspersky Total Security		Symantec Protection Suite Enterprise Edition	
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server					G Data EndpointProtection Enterprise plus PatchManagement					
Features: Management Server										
What is the maximum number of clients overall?	1000	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	25000	unlimited	unlimited
What is the maximum number of clients that can be managed from a single management server under the following conditions: All necessary components (database, repositories, update mechanisms, reporting, etc.) are installed on this server and the Clients communicate with the server either continuously or at least once per hour			50000	20000	1000		50000		80000	20000
Required <u>minimum</u> hardware (CPU/RAM/free disk space)	1GHz, 1GB RAM, 5GB disk space	No server hardware required. The server is hosted in-the-cloud.	1GHz, 512 MB RAM, 1GB disk space	2GHz, 1GB RAM, 6GB disk space	Core 2 Duo, 2GB RAM, 2,5GB disk space	2GHz, 1GB RAM, 500MB disk space	1GHz, 512 MB RAM, 1GB disk space	1GHz, 512MB RAM, 500 MB disk space	3GHz, 4GB RAM, 300GB	No server hardware required. The server is hosted in-the-cloud.
Does the product provide a mechanism to limit the data transferred over WAN Links when updating clients in remote locations?			*	*	*		*	*	*	
By designating one client as local source for definition updates (Super Agent, Group Update Provider)	*	*	*	*	*	*	*	*	*	
Which options does the product provide to ensure that only authorized administrators can administer the product?	username and password for authentication	Role based user models enforced through passwords	Password protection (role based management), encrypted communication	Password-based user authentication in Policy Manager Console.	Role based user model enforced through passwords / AD Login/Windows based Login / password-protected client / encrypted communication between server and client and server and administrative console	Password protection of the server	Authentication username, password, password-protected client, system tray icon hide	Password protection, encrypted communication, role-based administration	Symantec Authentication, Windows Authentication, and RSA Authentication	Administrator access is limited to those with a username and password plus an up to six-digit PIN number. Individual access rights are also imposed.
Log out administrator if idle for a specified time	*	*	*		*		*	*	*	*
Master-Slave-Server										
Multiple AV Servers	*		*		*		*		*	
Master server controls slave server in different offices	*		*		*		*		*	
Slave server for distributing updates	*		*	*	*	*	*		*	

Notes		Management server infrastructure is hosted in-the-cloud, providing High Availability and unlimited scalability. Individual Update Servers can be installed into LAN. It is possible to install and configure more Update Servers in cascade.	Slave servers can be nested in multiple levels, each with its own credentials for access, which can be dependent on administrator's role (read-only/limited user/full privileges). Policies from upper level servers could be propagated to lower levels.		Different deployment possibilities, such as: All in one management server deployment, redundant server deployment (Main and Secondary ManagementServer), combination between management server and cascaded subnet servers (Update agent) and/or Peer-to-Peer update distribution between clients, multiple management servers based for example on their location and managed with the G Data Master Administrator	every workstation/server with a simple windows fileshare can be used as a "distributing update server"	Update agent can be used for distributing updates. An Update agent is a PC within the Administration server network dedicated to store and distribute database updates, installation packages, group tasks and policies.			
<b>Client Installation</b>										
Which client deployment methods does the product support?										
Does the product include a mechanism that allows the administrator to push the software to the clients?	*	*	*	*	*	*	*	*	*	*
Can the installation of the clients be staggered over time to ensure that the network is not over utilized?	*		*	*	*		*	*	*	
Can the administrator see the status of the deployment (i.e. Transfer, Installation in Progress, Installation complete, etc.)?	*	*	*	*	*	*	*	*	*	*
Does the product include a mechanism that allows the end user to download and install the software?		*	*	*	*		*	*	*	*
Can the admin send a link which allows the user to download and install the software?		*	*	*	*	*	*	*	*	*
Does the product support the creation of MSI packages for deployment with 3rd party tools and Active Directory (GPO)?			*	*			*		*	*
Does the product support the creation of single file executable (.exe) installer (i.e. for logon scripts or CD distribution)		*	*	*	*	*	*	*	*	*
<b>Group Import &amp; Synchronisation</b>										
Can computers be imported from a text file?	*		*			*	*	*	*	
Can computers be imported from Active Directory?	*		*	*	*	*	*	*	*	*
Keeping the OU structure defined in Active Directory	*		*	*	*	*	*	*	*	*
Using other criteria to assign computers to groups	*		*	*	*	*	*		*	*
Can changes in Active Directory be synchronized?	*		*			*	*	*	*	*
Can the synchronisation schedule be defined?	*		*		*	*	*	*	*	
Can computers be imported from multiple Active Directory server?				*	*		*		*	*
Can computers/users be imported from other LDAP server?	*		*	*		*	*		*	
Can computers be imported by a GUI	*		*	*	*	*	*		*	
Can different actions be defined based on the malware category?			*		*	*	*	*	*	
<b>Scan Location</b>										
Can the administrator exclude/include files and folders from being scanned (by file extension)?	*	*	*	*	*	*	*	*	*	
By predefined lists of extensions provided by the product	*	*	*	*			*	*	*	
By filenames ("file.txt") regardless of folder or location	*			*	*	*	*	*		

[illegible]

Notify the end-user										
By displaying a pop up or balloon	*	*	*	*	*	*	*	*	*	*
Silent mode	*	*	*	*	*	*	*	*	*	*
By adding a warning to an infected email body or subject (email) and by replacing an infected attachment	*	*	*	*	*	*	*	*	*	*
Run a script or application after detection	*		*				*		*	
Can a second or alternative action be defined (i.e. if the first action fails)?	*	*	*	*	*		*	*	*	
Which file specific actions can the product perform?										
Clean / Delete	*	*	*	*	*	*	*	*	*	*
Can the product create a backup of the file before attempting to clean it?	*		*			*	*	*	*	
Quarantine on the local system	*	*	*	*	*	*	*	*	*	*
Quarantine in a central location			*	*	*		*	*	*	
Deny Access	*	*	*	*	*	*	*	*	*	*
Which processes specific actions can the product perform										
Terminate the process	*	*	*	*	*		*	*	*	*
Stop the service		*	*		*			*	*	*
Does to product provide preconfigured conditions?										
Preconfigured Antivirus Check		*	*			*	*	*	*	*
Preconfigured Firewall Check		*	*				*	*	*	*
Preconfigured Patch Management Check			*	*			*	*	*	
Other			Operating system patching status check				Database update		Operating system patching status check	
Remediation										
Does the product provide remediation capabilities?		*	*	*	*	*	*	*	*	*
Which remediation action can be defined in the user interface (without resorting to scripts)?										
Registry remediation				*			*	*	*	*
File remediation										
Delete files / folders		*	*	*		*	*	*	*	*
Download files							*	*	*	*
Process remediation										
Run service / application in user / system security context			*					*	*	*
Software Remediation										
Download software and patches			*	*	*		*		*	*
Install / uninstall software and patches in user / system security context				*	*		*	*	*	*
End-user interaction										
Inform user		*	*	*	*	*	*	*	*	*
Query user			*	*	*		*	*	*	
Enforcement										
Can the product prevent that a client failing the client health check connects to a network?				*			*		*	
Behaviour detection										
Behavior detection	*	*	*	*	*	*	*	*	*	*
Is this technology enabled by default?	*		*	*		*	*	*	*	*
General capabilities										
Is the firewall stateful for TCP and UDP connections?	*	*	*	*	*		*	*	*	*
Can the firewall analyze VPN traffic	*	*	*				*	*	*	*
Firewall Rules										
Does the product come with default policies?										
For workstations	*	*	*	*	*		*	*	*	*
For server		*		*	*		*		*	*
Protocol										
TCP/UDP/ICMP	*	*	*	*	*		*	*	*	*
Raw Ethernet		*	*				*	*	*	*
Other		Any other IP protocol is supported.	IPv6-ICMP, IGMP, GRE, ESP, SMP		IGMP, GGP, GUP, IDP, GRE					Processes and activity
Which Actions can be taken when a firewall rule is triggered?										

[illegible]

Is there a web based console?		*	*		*		*		*	*
Administrator Management										
Rights / Access Control										
Does the product support multiple administrators and different access levels?	*	*	*	*	*		*	*	*	*
Authentication mechanism										
Can administrators be authenticated using an integrated authentication mechanism (i.e. username / password)?	*	*	*	*	*	*	*	*	*	*
Does the product enforce minimum password lengths and maximum password age?		*	*	*	*		*	*	*	*
Can administrators be authenticated using Active Directory?			*		*		*	*	*	
Account Security										
Does the product log an administrator out after being idle for some time?	*	*	*		*		*	*	*	*
Administrator Auditing										
Does the product keep an audit log?		*	*	*		*	*		*	*
Device Control										
Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?			*	*	*		*	*	*	*
Failover										
What if the AV Server (local) hangs up										
automatic switching to a second local server		*	*		*		*	*	*	
updates from vendor-server instead of local server	*	*	*	*	*	*	*	*	*	
other			Log and notifications	Proxy pool and chaining		service is automatically restarted	any other network shared folder		Updates from another client (peer)	All servers are cloud based and fully redundant / worldwide
Quarantine										
Quarantine Folder										
Is there a centralized quarantine-folder			*	*	*		*		*	
Is there a quarantine-folder on the client	*	*	*	*	*	*	*		*	*
can administrators specify the location of the quarantine folder anywhere	*		*	*					*	*
rechecking quarantine										
after an signature update, is the quarantine folder checked?		*			*	*	*	*	*	
automatically		*				*	*	*	*	*
manual	*	*			*		*	*	*	*
undo av-action if false positive is detected		*				*	*		*	*
Messaging										
Exchange										
Feature overview Messaging										
Modules and functional areas		Monitoring, SMTP Groups, Antivirus, Antispam, Content filtering, Attachment filtering, Update	Product for Exchange. Full integration with MS Exchange, scans the whole Exchange store and Antispam Protection. Managable from the central management server. Supports 64-bit Exchange.	Transport and storage AV scanning, Spam Control, attachment filtering, intelligent file type recognition, keyword-based content filtering, zero-day protection, centralized quarantine management	Transport and storage AV Scanning and extendable by a MailSecurity Gateway		Anti-malware, anti-spam		Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Antispam, antivirus, antiphishing, content filtering, and data loss prevention	
Malware detection										
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled	*	*	*	*	*		*		*	
Information Store scan on every server	*	*	*	*	*		*	*	*	
Support of automatic virus pattern updates	*	*	*	*	*		*	*	*	
Scanning of e-mail message text and attachments	*	*	*	*	*		*	*	*	
Definition of file limitations by a combination of file name, file extension and file size	*	*	*		*		*		*	
Application of the restrictions on file archives	*	*	*	*	*		*	*	*	
Automatic detection of new mailboxes	*	*	*	*	*		*	*	*	



Scanning of existing mailboxes	*	*	*	*	*		*	*	*	
Anti-Spam										
scan according to the company's policies on prohibited, not desirable or confidential content	*	*	*	*				*	*	
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)	*	*	*	*			*	*	*	
Analysis of images on undesirable content (e.g. pornography)		*	*	*			*			
Using current spam pattern for the fast detection of new spammer tricks	*	*	*	*			*	*	*	
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails	*	*	*				*	*	*	
Definition of transmitter / receiver channels on a dedicated e-mail communications			*							
Freely editable exclusion list for addresses and content in subject and message text	*	*	*				*	*	*	
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email	*	*	*	*			*	*	*	
User-specific access to e-mails in the quarantine	*		*					*	*	
Centralized quarantine management	*	*	*	*	*		*	*	*	
Formation of company-specific e-mail categories	*		*						*	
Automatic classification of e-mails to one or more categories	*	*	*						*	
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees	*	*	*						*	
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined								*	*	
A content audit of e-mail attachments is also possible if the same mail is delivered several times, would it be blocked as spam			*					*	*	
		*	*							
Feature overview Messaging										
Modules and functional areas			Integration with most Windows mail servers is possible through the command line scanner		Gateway solution, Exchange Plugin for Exchange 2007/2010 or combination of both				Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Antispam, antivirus, antiphishing, content filtering, and data loss prevention	
Malware detection										
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled	*		*	*	*	*	*		*	
Information Store scan on every server	*		*	*	*			*	*	
Support of automatic virus pattern updates	*		*	*	*	*	*	*	*	
Scanning of e-mail message text and attachments	*		*	*	*	*	*	*	*	
Definition of file limitations by a combination of file name, file extension and file size	*		*	*			*		*	
Application of the restrictions on file archives such as zip, rar	*		*	*	*	*	*		*	
Automatic detection of new mailboxes	*		*	*	*	*		*	*	
Examination of encrypted e-mails for viruses in combination with Crypt					*					
Scanning of existing mailboxes	*		*	*	*	*		*	*	
Feature overview Messaging										

Modules and functional areas			Special product for Linux Mail Servers and Gateways. Includes Antispam, web administration interface. Managable from the central management console.		Windows-based Gateway Solution		Special product for Linux MTA (postfix, sendmail, exim, qmail, CGP). Includes Antivirus, Antispam and attachment filtering modules. Managable interfaces - Web and CLI.		Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Antispam, antivirus, antiphishing, content filtering, and data loss prevention	
Malware detection for messaging										
Anti-Spam										
Language:										
In which languages are your corporate products available?	German, English	English, French, Spanish, German	<b>Management Server and Console:</b> German, English, Spanish, French, Italian, Polish, Portuguese, Chinese, Japanese, Russian, Korean. <b>Client:</b> English, Slovak, Czech, Polish, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Bulgarian, Swedish, Danish, Finnish, Norwegian, Chinese, Slovenian, Ukrainian, Croatian, Italian, Estonian, Korean, Thai, Kazakh, Serbian, Japanese, Lithuanian.	Chinese, Czech, Danish, Dutch, English, Estonian, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish	German, English, Italian, Spanish, French, Russian, Polish, Turkish, Portuguese, Chinese, Japanese	German, English, French, Spanish, Italian, Chinese	English, Chinese, French, Italian, German, Japanese, Russian, Portuguese, Spanish, Turkish, Polish, Arabic, Korean, Vietnamese	English, French, German, Italian, Japanese, Spanish, Chinese	English, Chinese, Korean, French, Italian, German, Spanish, Portuguese, Russian, Czech, Polish, Japanese	Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish
In which languages are your (help) manuals available?			All		German, English, Italian, Spanish, French, Polish	German, English, Italian				English
Support										
24/7/365 phone support		*	*	*	*		*	*	*	*
Supported Support Languages	German, English	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French	German, English	All	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese	All
Remote Desktop Control for support	*	*			*	*		*	*	*
Support per Forum	*	*	*	*			*	*	*	*
Support over Email	*	*	*	*	*	*	*	*	*	*
On-Site service?		*	*	*	*	*	*		*	
Service										
Managed by Vendor, this means, can the whole management process be done as a service by the vendor?		*	*	*	*			*	*	
Pricing (may vary)										
Scenario A: 5 clients, server, outlook as mail client										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender	ESET Endpoint Antivirus	F-Secure Business Suite	G Data SmallBusiness Security	IKARUS anti.virus	Kaspersky Small Office Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection .Cloud	Webroot SecureAnywhere Business - Enterprise Protection
1 year Euro	267	143	150	306	167	34	167	214	120	132
3 years Euro	534	286	316	765	467	55	435	428	240	318
1 year USD	343	177	201	306	167	44	223	244	150	175
3 years USD	686	354	422	765	467	70	581	488	300	420

Scenario B SMB: 1 SBS 2003 Server, 25 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender	ESET Endpoint Antivirus + ESET File Security	F-Secure Business Suite	G Data EndpointProtection Business	IKARUS security.manager	Kaspersky Endpoint Security for Business SELECT	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Small Business Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	1260	556	473	941	570	910	810	656	684	452
3 year plan EURO	2520	1113	993	2263	1499	1456	1822	1312	1245	1086
1 year plan USD	1619	702	631	941	570	1170	1081	731	738	598
3 year plan USD	3238	1404	1326	2263	1499	1871	2433	1487	1343	1435
Scenario C: 1 Fileserver, 1 Exchange server, 200 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	9067	7476	4815	4818	8632	5454	10225	3950	5292	3210
3 year plan EURO	18135	14951	10113	12044	24536	8726	23004	7900	10079	7704
1 year plan USD	13390	9514	6430	4818	8632	7009	13658	4500	4944	4242
3 year plan USD	26780	19027	13503	12044	24536	11214	30728	9000	9310	10181
Scenario D, 2 Fileserver, 1 Exchange server, 1000 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	32011	29049	15821	15842	28960	19057	36914	18000	27075	12899
3 year plan EURO	64022	58097	33244	39600	81650	30491	83056	27000	61563	30958
1 year plan USD	47280	36387	21124	15842	28960	24492	49307	20250	20060	17051
3 year plan USD	94560	72774	44388	39600	81650	39187	110940	40500	44579	40923
Scenario E: 10 Fileserver, 10 Exchange server, 10000 Clients										
recommended product	Avira Small Business Security Suite	Cloud Security for Endpoints by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G Data EndpointProtection Enterprise plus PatchManagement	IKARUS security.manager	Kaspersky Total Security for Business	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Webroot SecureAnywhere Business - Enterprise Protection
1 year plan EURO	320110	216214	116084	81682	289600	120240	267067	180000	220820	105210
3 year plan EURO	742440	432428	243176	204204	816500	192384	600800	270000	530030	252504
1 year plan USD	470750	269272	154995	81682	289600	154530	356729	202500	159960	150300
3 year plan USD	1000000	538544	324688	204204	816500	247251	802507	405000	388788	360720

## Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (October 2013)